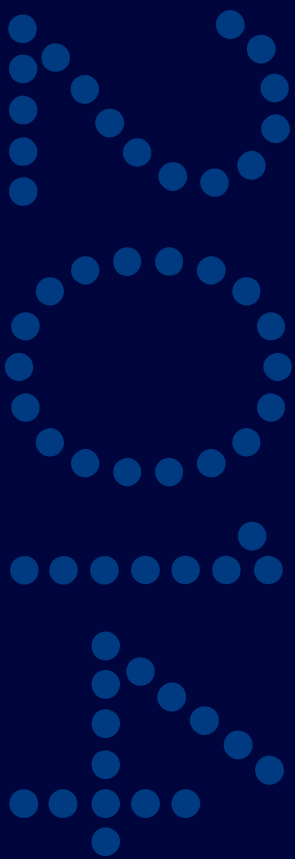
ANNUAL REPORT OF THE DATA PROTECTION COMMISSIONER OF IRELAND

Presented to each of the Houses of the Oireachtas pursuant to section 14 of the Data Protection Acts 1988 & 2003.



An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

TABLE OF CONTENTS

APPENDICES

HELEN DIXON
Data Protection
Commissioner of Ireland

FOREWORD

I'm delighted to present this, my first annual report as the Data Protection Commissioner of Ireland. I hope that it proves useful not just to both Houses of the Oireachtas, but also to the wider group of stakeholders with an interest both in our work and in data protection more generally. That wider group includes, of course, not just consumers, business people and other stakeholders across Ireland, but also a great many people across Europe and beyond. The nature of the internet means data protection is clearly a global matter, and I believe that meaningful cooperation and the free exchange of ideas are essential to making data protection work for everyone.

2014 has been a year of significant change for this Office. Billy Hawkes, an outstanding and highly respected Data Protection Commissioner, stepped down after nine years of excellent and insightful service. I'd like to acknowledge the crucial role he played in guiding the development of data protection in Ireland, while working closely with counterparts in other countries. Billy and his team also worked hard to build the capabilities of our Office, paving the way for a near-doubling of the 2015 budget from €1.8m to €3.65m, a rapid growth in headcount in 2015 from 29 to 50, and the opening of a new office in Dublin in 2015.

I came into the post in the autumn of 2014, following a public, competitive and independent process run by the Public Appointments Service of Ireland. Underlining the international aspect of my Office, the head of a fellow European Union data protection authority sat on the interview board (Christopher Graham, the Information Commissioner of the United Kingdom). 2014 also saw the Irish government appoint, for the first time, a Minister with a specific brief for data protection (Dara Murphy, TD, Minister of State with Special Responsibility for European Affairs and Data Protection). While I and my Office operate fully independently of the Irish government – and indeed are independent, full stop – Minister Murphy's appointment confirms once again the growing importance of data protection and its cross-border nature.

Data protection is, you will be unsurprised if I tell you, a very fast-moving field. The ways in which data can be collected, analysed, stored, used and abused are all constantly changing, in ever-smaller units of time, and affecting ever-greater numbers of people. In Ireland, smartphone penetration is now at 59% of the subscriber market, use of geolocation data is commonplace and we routinely conduct banking transactions online. Given the pace and scale of change, I believe it is essential for data-protection authorities to have strong relationships with stakeholders, and regular meaningful dialogue.

The engaged approach adopted by my Office means data-protection problems can be detected, and either solved or eliminated, before they affect a greater number of people than would otherwise be the case. It is better for a regulator to be talking to companies and suggesting improvements to borderline compliant products and services before they reach the market, than to see those products launched and to act only once consumers and other stakeholders have already been affected. Engagement also means that an independent regulator,

The ways in which data can be collected, analysed, stored, used and abused are all constantly changing.

such as my Office, is better able to guide meaningfully and consistently, over time, the broader development of data protection for the improved benefit of all parties.

Sometimes, of course, effective data-protection regulation is best carried out through the use of our statutory powers. This report illustrates the occasions when effective data-protection regulation means issuing, for instance, Statutory Enforcement Notices or examining Data-Breach Notifications, or carrying out a privacy audit (organisations we investigated under the terms of a privacy audit in 2014 included LinkedIn and An Garda Síochána, the Irish police force). While the explicit use of these tools can be measured, as they are in this report, the implicit threat of their use to ensure compliance is also very useful, though necessarily harder to capture statistically.

I took up my post as Data Protection Commissioner of Ireland following a period in which Ireland has become home to the European headquarters of many of the world's leading technology companies. Given the nature of European Union data-protection legislation, this means that my Office plays a key role in regulating the activities of such companies not just in Ireland, but across the European Union. The responsibility that I and my Office owe to people across the European Union calls, I firmly believe, for the engaged approach I have outlined above, to ensure their data-protection rights are upheld while ensuring access to digital services that many enjoy and even rely upon. There are those that disagree with this approach, and there are discussions afoot about the underlying framework of data protection in Europe. But with the framework and the facts as they are, I am confident that the engaged approach used by my Office is the right one, and that our expanded resources and geographic proximity to decision-makers in leading technology companies make us well-placed to regulate with the full efficacy that our stakeholders deserve.

The responsibility that I and my Office owe to people across the European Union calls, I firmly believe, for the engaged approach, to ensure their data-protection rights are upheld while ensuring access to digital services that many enjoy and even rely upon.

In terms of the European framework for data-protection regulation, my Office and I are closely following negotiations around the new General Data Protection Regulation – which is expected to provide a more harmonised data-protection law. Whatever shape this takes, effective data protection in Europe will continue to demand close cooperation between stakeholders, including, of course, fellow data-protection authorities in different countries. We must all be open to suggestions – and helpful criticism – while remembering that we share the same overarching goal of effective data protection, and continuing to maintain the trust and goodwill upon which European cooperation always depends.

2014 provided further reminders of the significance of the Court of Justice of the European Union in relation to data protection. The year saw a decision in the Google Spain case – which recognised a so-called "right to be forgotten" – and the effects of that decision continue to play out. A case centred around personal data transfers outside the European Economic Area was referred by the Irish High Court to the CJEU, and we look forward to the outcome of this case as an event of significance with regard to data regulation by European authorities.

2014 also saw significant cooperation between my Office, the Canadian Commissioner and the Office of the Australian Information Commissioner and the Federal Trade Commission with regard to a data breach by Adobe. The memoranda of understanding my Office has in place with these authorities proved highly useful, leading to much more rapid outcomes than might otherwise have been the case.

While our expanded international remit has given my staff and me plenty to do, 2014 was also a busy year in terms of work relating principally to Ireland. We were involved in a consultative capacity in many large-scale government projects, which is an effective way to ensure data protection is built into these kinds of projects from the outset. My staff and I took a role in a consultation about the government's proposed Data-Sharing and Governance Bill, regarding lawful data-sharing between public bodies. We began 2015 by continuing to input into this proposed legislation, with the goal of ensuring adequate safeguards

The prosecutions were ground-breaking, as they saw the use of Section 29 of the Data Protection Acts of 1988 and 2003 to prosecute the directors of a given company for their part in breaches by investigators employed by the company.

and adherence to data-protection principles remain central to the proposals.

Challenges to the use of the Personal Public Service Number by the new water utility, Irish Water, led to a large volume of work in dealing with queries and investigating complaints. A legal basis for Irish Water to collect and process the PPSN existed but citizens wanted to understand the details around this, such as why the PPSN was being collected, what authority the utility had to collect it, what purposes it would be used for, with whom it would be shared and how long it would be retained. Broadly, the scenario provided a reminder to organisations that information about data collection and use needs to be clear and precise, otherwise confusion and disquiet may be the result. We fielded similar queries and complaints about the Department of Education and Skills Primary Online Database. The Department has made a number of amendments and ameliorations in relation to the project, particularly with regard to the explanatory material prepared for parents. As 2015 began, we remained engaged with the Department about these matters.

Last year's annual report of the Commissioner highlighted our work with regard to the proposed "Eircode" national postcode system. Due to be rolled out in mid-2015, this provides a unique and randomised code for each household (that is, each individual house or apartment), and as such it represents a unique identifier for each household address. It is clear (particularly in light of the rate of single-occupancy households in Ireland) that the Eircode should be regarded as personal data, under the definition in the Data Protection Acts 1988 and 2003. While it is true that, on its own, Eircode is merely a unique identifier for an address and not a person, it is equally the case that in most contexts of its envisaged usage, a data controller will likely have additional information that would then allow identification of an individual person. The Data Protection Commissioner advised the Department of Communications, Energy and Natural Resources to underpin the Eircode project with specific primary legislation. The Department accepted this advice and is now advancing the project with built-in legislative safeguards to protect privacy.

In terms of the prosecution work of this Office, 2014 saw us undertake a high volume of casework in relation to private investigators (also known as tracing agents). We uncovered significant issues across the sector in terms of abuse of personal data – a more complete outline of our actions is detailed later in this report. The prosecutions were ground-breaking, as they saw the use of Section 29 of the Data Protection Acts of 1988 and 2003 to prosecute the directors of a given company for their part in breaches by investigators employed by the company. The prosecutions sent a strong message to data controllers that they must carry out better diligence before hiring a private investigation firm to process personal data on their behalf, and also to state data controllers that they must ensure they are not inadvertently leaking personal data to third parties.

Self-reported notifications of data breaches to the Office remained high in 2014, at nearly 2,300 during the year. The principal causes of data breaches were human error and not systemic, such as the inclusion of the wrong bank statement in the wrong envelope, or the attachment of the wrong spreadsheet to an email.

2015 sees this Office in a stronger-than-ever position to continue, in Ireland and beyond, helping to shape the data-protection environment and ensuring proper compliance with the relevant laws. I look forward to continuing to engage warmly and constructively with my European and global counterparts, fully reflecting the cross-border nature of data protection. 2014 saw the beginning of significant change for the Office of the Data Protection Commissioner of Ireland, and this transformation will continue during 2015.

HELEN DIXON,
Portarlington and Dublin, 23 June 2015

ROLE AND RESPONSIBILITIES OF THE DATA PROTECTION COMMISSIONER OF IRELAND

- The Office of the Data Protection Commissioner (DPC) came into being in 1989 following the enactment of the Data Protection Act of 1988. The early issues that the Office dealt with focused on the financial sector – however, the range of issues we deal with has greatly expanded over the last quarter of a century, as has our responsibility to Irish and EU service users.

- The Office of the Data Protection Commissioner is an independent body, which derives its power and authority from the Data Protection Acts 1988 and 2003, which were enacted to give effect to the 1981 Council of Europe Convention and the later 1995 EU Data Protection Directive.

- Funding for the Office of the Data Protection Commissioner is secured through the vote of the Irish Department of Justice and Equality, so, in effect, all funding for the Office comes from the Irish exchequer. The DPC collects revenue from the statutory registration function of the Office, and the revenue is remitted directly back to the exchequer. The government has significantly increased funding to the DPC for 2015 and its annual budget now stands at €3.65m.

- While the Office of the Data Protection Commissioner is an independent body, and has publicly made decisions and enforced against government and industry alike, it is not without oversight in relation to its administration. All expenses, costs and expenditure must be accounted for to the exchequer, and the DPC accounts come under the Comptroller and Auditor General's remit. In addition, as the Office has a large public-facing function in examining complaints raised by individuals, and interacts daily with citizens and businesses, these key stakeholders provide a type of oversight of the Office's work. In relation to statutory decisions of the Office, these can be appealed to the courts.

- The Office of the Data Protection Commissioner's primary goal is to drive compliance with legislation that requires the safe collection, storing and processing of individuals' personal information. The Office examines complaints from individuals who assert that their data-protection rights have been contravened and may enforce against organisations that commit offences under the Acts. The Office actively monitors the constantly changing landscape of data protection and provides and updates guidance to individuals and organisations. With the arrival of large multinational corporations in Ireland, collecting and storing vast amounts of data, the Office acts as a bulwark against possible misuse or disclosures of personal information and ensuring compliance with the Data Protection Acts.

- The Office continues in its role as "lead regulator" of an increasing number of multinational technology companies who are principally headquartered in the US but have chosen to declare Ireland as their European headquarters, following the suite of companies like Apple and Intel, who have been based in Ireland for decades. Due to the manner in which these companies are structured and the way in which EU data-protection law has been applied regarding establishment, jurisdiction and data controllership, the operations of these companies have been regulated from a data-protection perspective by the Irish Data Protection Commissioner, even when they operate in many EU countries and process the personal data of European citizens. On foot of a recent European Court of Justice decision on establishment for non-EU based data controllers, the concepts of "main establishment" and "applicable law" are now subject to debate. Also, the proposed "one-stop-shop" mechanism for dealing with large multinational operations among data-protection authorities in Europe has yet to be finalised as part of the General Data Protection Regulation (GDPR), which will supersede EU Directive 95/EC/46. It is hoped that the General Data Protection Regulation will provide clarity on these crucial issues.

- European Role – Article 29 of the 1995 EU Directive establishes a "Working Party on the Protection of Individuals with Regard to the Processing of Personal Data". It is made up of a representative from the data-protection authority of each EU member state, including the Irish Data Protection Commissioner. The Working Party is independent and seeks to harmonise the application of data-protection rules throughout the EU, and publishes opinions and recommendations on various data-protection topics. It also advises the EU Commission on the adequacy of data-protection standards in non-EU countries. As a member of the Working Party, the Irish Data Protection Commissioner pro-actively contributes to the overall regulatory picture, both in Europe and on the international stage.

The Data Protection Commissioner lists her immediate goals as being:

1. To expand and build the capacity and capability of the data-protection authority in Ireland through procuring additional resources and recruiting additional staff.

2. To establish a Dublin-based presence of the data-protection authority, which will work in conjunction with the existing Portarlington office.

3. To improve the customer service, website and communications functions of the DPC.

4. To drive better compliance with data-protection legislation by the Irish public sector.

5. To improve international cooperation by the Irish DPC, in particular with its Article 29 "Working Party" counterparts.

REVIEW OF 2014 IN BRIEF

- We dealt with 13,500 queries via our dedicated information email address, info@dataprotection.ie, an increase from 12,000 in 2013. In addition we dealt with enquiries received by phone and post.
- We received 960 complaints, which were opened for investigation. This compares with 910 complaints open for investigation in 2013.
- The largest single category of complaints related to access requests, which accounted for just over half the total, reflecting public awareness regarding the right of access to data held about them.
- The second largest category of complaints concerned electronic direct marketing.
- While the vast majority of complaints were resolved amicably, we made formal decisions in 27 cases, 18 of which fully upheld the complaint.
- A new category of complaint emerged in 2014, relating to internet search result delisting, following the Google Spain case – we received 32 such complaints against search engines.
- We prosecuted 9 entities for a total of 162 offences under the Data Protection Acts of 1988 and 2003, and the Privacy in Electronic Communications Regulations of 2011.
- While the vast majority of organisations engage voluntarily with us, we issued three Statutory Enforcement Notices.
- We received 2,264 data-security breach notifications, an increase of 681 on the previous year.
- Enforced Subject Access Requests – whereby job applicants are required to source personal information about themselves from organisations such as An Garda Síochána – became an offence in 2014, and we have worked to combat this practice.
- We carried out 38 audits and inspections, prioritising multinational technology companies and major public-sector organisations.
- We finalised our audit of LinkedIn-Ireland, and our audit of An Garda Síochána was published.
- We engaged with large tech multinationals, with headquarters or significant presences in Ireland, regarding numerous matters, such as proposed new products and services and emerging data-protection issues.
- We published a revised **Guide to the Audit Process**.
- We approved new Data Protection Codes of Practices with the Probation Service and with the Department of Health.
- In April 2014, the Court of Justice of the European Union (CJEU) found that the 2006 Data Retention Directive was invalid, leading a number of European Union states to amend their legislation in this area.
- May 2014 saw the CJEU issue judgment in the Google Spain case, giving rise to significant changes in the data-protection environment in Europe with particular regard to search engines.
- December 2014 saw the CJEU issue judgment in the Rynes case, relating to data and domestic CCTV usage.
- The Commissioner or the Deputy Commissioner attended all plenary meetings of the Article 29 Working Party, which acts as an advisor to the European Union on data-protection issues.
- We took part in the second Global Privacy Enforcement Network Privacy Sweep, analysing 20 apps for data and privacy issues.
- We created and ran a series of presentations for second-level students on cyber awareness and privacy around apps.
- Our running costs in 2014 were €2,274,438, an increase from €1,960,999 the previous year. Receipts from fees increased to €714,697 from €647,997.
- We dealt with over 500 enquiries from the media.
- In October 2014, we began a new Irish language scheme, under the Official Languages Act 2003, and continue to provide an Irish language service, as well as Irish language information via our website www.cosantasonrai.ie.
- The Freedom of Information Act 2014 came into effect in October of 2014. From 14 April 2015, the Office of the Data Protection Commissioner (DPC) became partially subject to the Freedom of Information Act 2014.

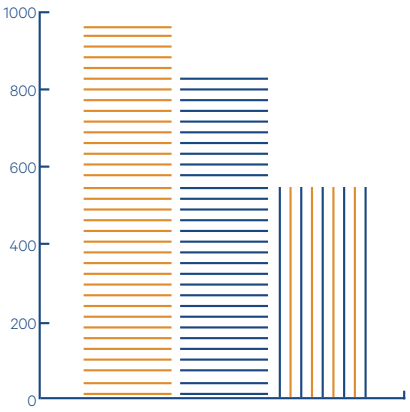
COMPLAINTS RECEIVED

During 2014, the Office received 960 complaints, which were opened for investigation. This compares with 910 complaints in 2013.

Once again, the largest single category of complaints related to access requests. This category of complaint accounted for 54.3% of the overall total for 2014, with 521 complaints topping the high record set in the previous year (517 complaints were received in this category in 2013). As noted in previous reports, the high level of complaints with regard to access requests is indicative of the increased level of awareness among the general public of their statutory right of access and it also points to the extent of the difficulties being experienced by some individuals in their efforts to exercise their rights and the barriers that some data controllers place in their way.

The second highest category of complaints concerned electronic direct marketing. These complaints are investigated under the Privacy in Electronic Communications Regulations (S.I. 336 of 2011). In 2014, the Office opened 176 such complaints for investigation (18.3% of the overall total). This is a decrease of 28 complaints compared with 2013. These complaints related to unsolicited direct-marketing text messages, telephone calls, fax messages and emails. Significantly, this is the first year since 2005 that complaints in this category dropped below 200 in a calendar year. This is a welcome development, particularly when we recall that electronic direct-marketing complaints hit an all-time high in 2007 when the Office received 538 such complaints – which was over three times higher than the 2014 total. The Office is confident that its active prosecution strategy in this area has contributed to the overall decline in this category of complaint.

The vast majority of complaints concluded in 2014 were resolved amicably through the efforts of the Office without the need for a formal decision under Section 10 of the Acts. We are obliged to seek to attempt to amicably resolve complaints in the first instance. In 2014, the Commissioner made a total of 27 formal decisions: 18 of these fully upheld the complaint, 2 partially upheld the complaint and 7 rejected the subject of the complaint. A total of 829 investigations of complaints were concluded in 2014.



2014	
Complaints opened in year	960
Total complaints concluded in year	829
Total complaints at end of year	549

Table 1 shows the breakdown of complaints by data-protection issue. Excluding the 176 complaints (approx. 18.3%) concerning alleged breaches of S.I. 336 of 2011, the other 784 complaints (approx. 81.7%) relate to alleged breaches of the Data Protection Acts 1988 and 2003. Table 2 gives details of the number of complaints received on an annual basis since 2005.

Table 1
Breakdown of complaints by data protection issue 2014

	Percentages	Totals
Access Rights	54.3%	521
Electronic Direct Marketing	18.3%	176
Disclosure	7.2%	69
Unfair Processing of Data	5.0%	48
Internet Search Result Delisting	3.3%	32
Use of CCTV Footage	3.0%	28
Excessive Data Requested	3.0%	28
Unfair Retention of Data	1.6%	15
Accuracy	1.1%	11
Failure to secure data	1.0%	10
Postal Direct Marketing	0.9%	9
Right of Rectification	0.5%	5
Other	0.8%	8
TOTALS	**100.0%**	**960**

Table 2
Complaints received since 2005

Year	Complaints Received
2005	300
2006	658
2007	1037
2008	1031
2009	914
2010	783
2011	1161
2012	1349
2013	910
2014	960

A new category of complaint emerged in 2014 – Internet Search Result Delisting – arising from a ruling of the Court of Justice of the European Union (CJEU) on 13 May 2014 in the case of Google Spain v AEPD and Mario Costeja (Case C-131/12) (commonly known as the "Google" Spain ruling). This ruling confirmed the application of data-protection law to search engines and it also concluded that users may request search engines, under certain conditions, to remove the links to information affecting their privacy specifically where a search has been conducted on the name of that individual. Where a search engine refuses a request, the data subject may bring the matter before the data-protection authorities of the European Union. The Article 29 Working Party in November 2014 issued guidance and proposed criteria to its member countries and to search engines in terms of deciding how the Google Spain ruling should apply to delisting scenarios. In 2014, the Office received 32 such complaints against search engines.

Prosecutions – the Office prosecuted nine entities in 2014 for a total of 162 offences, spanning both the Data Protection Acts 1988 and 2003 and the Privacy in Electronic Communications Regulations (S.I. 336 of 2011). The Case Studies section of this annual report carries further details of the prosecutions taken in 2014.

STATUTORY ENFORCEMENT NOTICES

Under Section 10 of the Data Protection Acts 1988 and 2003, the Data Protection Commissioner may require a data controller or data processor to take whatever steps the Commissioner considers appropriate to comply with the terms of the Acts.

Details of Statutory Enforcement Notices served in 2014 are set out in the following table. Most relate to the right of access. It is hoped that publication of these lists encourages all organisations that are the subject of complaints to cooperate fully with this Office in relation to its statutory investigations.

While an Enforcement Notice may be issued in relation to a number of aspects of the Data Protection Acts, it is not normally necessary to do so. The vast majority of organisations voluntarily engage with the Office without the need for a formal legal notice to advance an investigation.

Enforcement Notices issued in 2014:

Data Controller:	In relation to:
Kevin P. Kilrane & Co	Section 4(1) of the Data Protection Acts
Paddy Power Plc	Section 2(1)(d) and Sections 2C(1)(b)(i) and (ii) of the Data Protection Acts
Toplook Salon	Section 4(1) of the Data Protection Acts

SELECTED INFORMATION NOTICES

Under Section 12 of the Data Protection Acts 1988 and 2003, the Data Protection Commissioner may require a person to provide her with whatever information the Commissioner needs to carry out her functions, such as to pursue an investigation. Below is a list of Selected Information Notices issued in 2014.

Data Controller:
Truck Plant Mobile Services Limited
ESB Electric Ireland Limited
Health Service Executive (PCRS)
Sixmilebridge Credit Union Limited
St Paul's Garda Credit Union Limited
Blackpool Credit Union Limited
Glanmire and District Credit Union Limited
Ballinlough Credit Union Limited
Mitchelstown Credit Union Limited

DATA-BREACH NOTIFICATIONS

During 2014, the Office received 2,264 data-security breach notifications. The Office considered that 76 such notifications were not classified as data-security breaches, under the principles of the **Personal Data Security Breach Code of Practice**. A total of 2,188 valid data-security breaches were recorded.

This is an increase of 681 on the previous year. The increased numbers are accounted for by a large increase in the number of data-security breaches through disclosures made via postal and electronic means. The majority of mailing breaches being reported to the Office come predominantly from the financial sector, which accounts for two thirds of such notifications. The breaches are caused by a number of issues, such as third-party data being inadvertently included in correspondence, addresses being incorrectly recorded at time of collection, or data being issued to brokers not acting on behalf of the affected individual. There are other data-security breaches that are caused by technical issues, but the majority relate to simple human error. The impact such data-security breaches have on affected individuals varies. In many cases, the breach poses a low risk to individuals. In some cases, though, there is a cause of embarrassment to the affected individual when the correspondence relates to outstanding debts and, in limited cases, inappropriate access to account information. The data controller usually becomes aware of the issue when they are notified by the third-party recipient. The data controller will then seek either the return of the documents or confirmation that the documents will be destroyed

The Office has been contacted by a number of individuals who have received notification from a financial institution of a disclosure of their personal data. A concern that they express is the fact that they do not know who has received such information about them. The data controller cannot release the name and address of the recipient of their data as this would be a further disclosure of personal data. The data controller can only advise that they have either secured the return of the documents or received assurance that the documents have been destroyed. The data controller must also have appropriate security arrangements in place to ensure that any individual contacting them must be able to verify their identity before being allowed access to account data.

These breaches usually impact only one or two individuals at a time. The Office receives many notifications from other types of data controller that can impact several thousand individuals at a time. In certain cases, the data controller can have a presence in multiple jurisdictions, and this Office will liaise with the relevant data-protection authorities in other jurisdictions to conduct an investigation into the data-security breach. One example of such an investigation is the data-security breach notification received from Adobe in October 2013. The number of individuals affected by this particular breach was in the millions. This Office entered into a joint investigation of the matter with the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner, the findings of which were recently published. The US Federal Trade Commission was also consulted during the investigation. The Office has also received requests for assistance in investigating issues from other jurisdictions seeking information regarding data controllers based in Ireland. This Office is committed to providing assistance to our counterparts in other jurisdictions to ensure that data-protection rights are enjoyed by all.

Due to the geographic spread of customers of large data controllers, a data-security breach can affect individuals across many jurisdictions. It is encouraging to know that data-protection authorities can work together, sharing their knowledge and experience, in investigating such security breaches to ensure the rights of the individual are protected. The Office worked closely with the Office of the Privacy Commissioner of Canada and the Office of the Australian Information Commissioner during the investigation of the Adobe data-security breach and we thank them for their invaluable assistance in this matter. We also thank the US Federal Trade Commission for its input into this matter.

We have received notification of issues from third parties who happen across potential breaches of data-protection rights. In one case last year, we were notified of a website that appeared to be hosting documents containing the name, address and PPSN of approximately 38,000 individuals. The website was hosted in Eastern Europe. When the Office examined the website, it appeared to contain a list of valid names, addresses and PPSNs. Upon investigation, it appeared that the file was created in 2009. We contacted both the Revenue Commissioners and the Department of Social Protection, seeking their assistance in the matter. We provided them with a copy of the data hosted on the website and asked if they could identify the source of the data. Both reported that while some of the names and addresses were valid, the PPSNs were not valid numbers. We then contacted the hosting company for the website and requested that the relevant data be taken down. The data was subsequently removed from the website.

The attached tables provide a breakdown of the notifications received.

Number of Breach Notifications Received, 2014

Total Number of Breach Notifications Received	2264
Number Considered as Non-breach	76
Number of Breach Notifications	2188

Number of Organisations Making Breach Notifications, 2014

Private-Sector Organisations	254
Public-Sector Organisations	60

Breach Notifications – by Category

Category	Number
Theft of IT Equipment	41
Website Security	34
Mailing Breaches (Postal)	1318
Mailing Breaches (Electronic)	274
Security-related Issues	153
Other	368
Total	**2188**

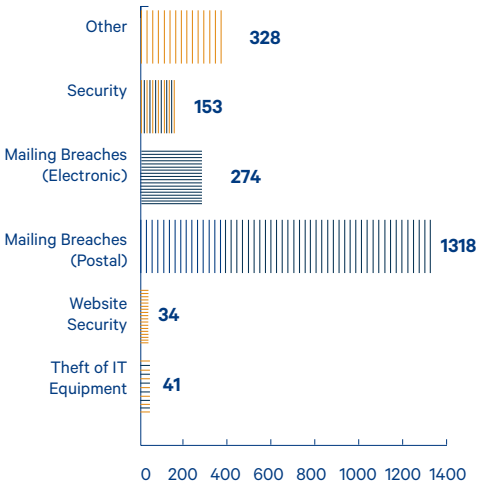
Comparison of Breach Notifications – by Year

2010	410
2011	1167
2012	1592
2013	1507
2014	2188

Comparison of Organisations making Breach Notifications

Year	Private	Public Sector	Total Sector
2010	89	34	123
2011	146	40	186
2012	220	84	304
2013	246	61	307
2014	254	60	314

Breaches by Category



ENFORCED SUBJECT ACCESS REQUESTS

An "enforced subject access request" is where an applicant is obliged by a potential employer or organisation they are dealing with to make an access request under Section 4 of the Data Protection Acts to a data controller. The individual is typically then asked to provide this information to their employer/prospective employer/ recruitment agency.

The Data Protection Commissioner advises all data controllers and processors that enforced subject access is now an offence. In 2014, the Minister for Justice and Equality signed Statutory Instruments 337 and 338, bringing the remaining sections of the Data Protection Acts into force with effect from 18 July 2014, including Section 4(13) of the Acts.

With Section 4(13) of the Data Protection Acts in force, it is therefore now unlawful for employers to require employees or applicants for employment to make an access request under Section 4 of the Data Protection Acts. It also applies to any person who engages another person to provide a service such as a recruitment agency or pre-screening organisation. An employer who requires an employee or prospective employee to make such an access request commits a criminal offence under the Data Protection Acts.

In 2015 and onwards, the Data Protection Commissioner intends to vigorously pursue and prosecute any abuse detected in this area. Section 4(13) of the Data Protection Acts states:

(a) A person shall not, in connection with —
  (i) the recruitment of another person as an employee,
  (ii) the continued employment of another person, or
  (iii) a contract for the provision of services to him or her by another person, require that other person —
    (I) to make a request under subsection (1) of this section, or
    (II) to supply him or her with data relating to that other person obtained as a result of such a request.

(b) A person who contravenes paragraph (a) of this subsection shall be guilty of an offence.

In the UK, similarly Section 56 of the UK Data Protection Act 1998 (DPA) has commenced in early 2015 whereby it is a criminal offence for employers to require a candidate or current employee to use his or her subject access rights under the UK Data Protection Acts to obtain and then provide certain records to the employer as a condition of employment.

Section 4 Access Requests to An Garda Síochána

In the case of access request applications to An Garda Síochána, information released under an access request should not be considered as a formal Garda vetting procedure for employment or other purposes.

Garda vetting is mandatory under legislation such as the Child Care Act 1991, the Child Care Regulations 2006 and the Teaching Council Act 2001. Vetting also takes place in relation to certain state employees working in sensitive areas and to persons working in the private-security industry; these are covered by the Private Security Services Acts (nightclub security staff etc.). In 2014, there were over 320,000 vetting applications processed by the Garda Central Vetting Unit.

As part of the follow-up to the audit of An Garda Síochána (report published March 2014), the Office of the Data Protection Commissioner is monitoring the number of access requests made under Section 4 of the Acts to the Data Protection Processing Unit. As per the audit report of AGS, it was noted that the Data Protection Processing Unit received 11,266 access request applications in 2012. In 2014, a very similar number was recorded: 11,219.

The Office of the Data Protection Commissioner considers these access request figures to be questionably high in terms of the number of individuals actively invoking their data-protection rights by making such requests to An Garda Síochána. Of concern is the real prospect that organisations who would not legitimately qualify to conduct a vetting check would instead turn to Section 4 of the Data Protection Acts and, in effect, engage in "vetting by the back-door". Even more alarming is the fact that a Section 4 access request could potentially reveal a lot more sensitive data than would ever be disclosed on foot of a legitimate vetting check.

A Section 4 access request could result in everything held on Garda records about a person being disclosed (subject to certain exemptions under Section 4 and 5 of the Data Protection Acts). This is chiefly because the data disclosed is intended to be for the information of the person making the request only.

A vetting check has always been subject to certain restrictions on what would be disclosed. In a recent further development, on 31 March 2014, the Minister for Justice and Equality implemented an "administrative filter"[1] to be applied to all Garda vetting applications. The administrative filter is a new procedure being applied by the Garda Central Vetting Unit to allow certain minor convictions over seven years old to be removed from disclosures. The Office will continue to monitor this area following the commencement of Section 4(13) of the Data Protection Acts.

PRIVACY AUDITS

The Commissioner is empowered to carry out privacy audits and inspections to ensure compliance with the Acts and to identify possible breaches. Scheduled audits are intended to assist the data controller in ensuring that their data-protection systems are effective and comprehensive, and are sometimes supplementary to investigations carried out by the Office in response to

1. http://www.garda.ie/Documents/User/Garda%20Vetting%20Procedures%20-Aministration%20Filter%20revised.pdf

specific complaints. Priorities and targets for audit are identified, taking account of factors such as the amount and nature of personal data processed by the organisation and complaints and enquiries to the Office. A particular priority is given to multinational technology companies with establishments in Ireland and to major holders of personal data in the public sector. In the course of the year, 38 audits and inspections were carried out. In addition, a desk-based audit of 20 mobile apps was conducted as part of a Global Internet Privacy Sweep themed "Mobile Privacy". The Office also continued with its programme of unscheduled inspections under powers conferred under Section 24 of the Data Protection Acts.

In August 2014, a revised **Guide to the Audit Process** was published. This guidance was originally published in 2009. The revised version was updated to take account of subsequent legislative developments and to reflect any changes in the approach of the Office of the Data Protection Commissioner to the audit process.

As in previous years, the programme of audits was tailored to allow for a focus on a few carefully selected targets; in 2014, this entailed a focus on the finalisation of the LinkedIn-Ireland audit report based on the 2013 audit of LinkedIn-Ireland and the publication by An Garda Síochána of the audit report on www.garda.ie.

One area selected for particular attention in 2014 was the data-processing activities of credit unions, private investigators, accountants and liability adjusters. All of these entities were targeted on the basis of the ongoing investigation by the Office into inappropriate access to state databases by agents appointed by organisations engaged in the pursuit of debts. Insurance companies and other financial institutions will be the subject of such scrutiny by the Office in the future with regard to their use of private investigators to examine potentially fraudulent insurance claims.

In terms of the public sector, an emphasis was placed on citizen-facing services such as a motor tax office, a recently established National Driver Licence Service Centre, a Money Advice & Budgeting Service, a Citizens Information Centre and the HSE's customer complaints service "Your Service Your Say".

One of the largest data brokers in the state was audited in order to ensure its compliance with the principles of fair obtaining and processing as well as direct-marketing regulations. The audit team also embarked upon a programme of audits of shopping centres, with specific regard to CCTV cameras and the requirement for a CCTV policy to be in place. Another area of focus was the beauty and cosmetic sector in which a large beauty clinic chain and a slimming company were selected for audit. In all cases, the Office had the opportunity to issue a range of recommendations customised to each organisation; all displayed a willingness to meet the requirements of these recommendations. In terms of sectoral engagement based on audit findings, the Office is meeting with representatives of retail bodies in order to further address issues identified during the targeted programme of audits in shopping centres.

LinkedIn-Ireland

In 2013, a major audit of LinkedIn-Ireland (LI-I) commenced. The on-site element of the audit was conducted in May 2013 in LinkedIn-Ireland's European headquarters in Dublin. Intense systems testing and interaction with the company continued throughout 2013 and into 2014. The audit report of LinkedIn-Ireland was finalised in July 2014 following detailed discussion and clarification with LI-I.

As part of the Office's ongoing engagement with other European data-protection regulators, the preparation of the report entailed consultation within the Article 29 Working Party and its Technology Subgroup mechanisms, the membership of which comprises a representative from the data-protection authorities of each EU member state, the European Data Protection Supervisor and the EU Commission. This engagement took place in order to ensure that any particular concerns of individual data-protection regulators could be accommodated. The Office continues to engage with LI-I concerning progress on implementation of the recommendations in the report, and this dialogue will continue in 2015.

The Office of the Data Protection Commissioner has established a scope-and-risk basis for audits of the many other multinational technology companies with establishments in Ireland. This approach balances the resources and skills required with the needs of other investigations into particular technology issues that arise during the normal course of operations within the Office.

An Garda Síochána

In February 2014, An Garda Síochána published the report of the data-protection audit carried out by the Office.

The audit consisted of an examination of documentation provided by An Garda Síochána, on-site inspections at An Garda Síochána HQ in Dublin, the Garda Síochána Vetting Unit in Thurles, the Garda Síochána Information Services Centre (GISC) in Castlebar and a number of Garda stations. A central focus of the audit was the main IT system used by An Garda Síochána for recording data, PULSE, as the initial phase of the audit had uncovered some evidence of inappropriate access to PULSE by members of An Garda Síochána. The audit findings highlighted areas where improvements are required. Overall, the majority of areas examined demonstrated professionalism on the part of the Garda force in terms of operating in compliance with data-protection legislation. The Office continued to engage with An Garda Síochána throughout 2014 in terms of the implementation of the recommendations and notes the good progress that has been made in this regard.

GUIDANCE, BINDING CORPORATE RULES, AND CODES OF PRACTICE

Guidance
During 2014 the Office provided guidance and advice about data protection to a wide range of public and private organisations. Over 120 consultations took place, each of which involved varying degrees of interaction with this Office. Providing guidance in this way helps organisations to ensure compliance with the Data Protection Acts from the inception of their policies and business initiatives, and we often continue to advise as projects are rolled out.

Projects we consulted on during 2014 included:

- The Credit Reporting Act
- The Health Information Bill
- Sports Ireland Bill
- Credit Reporting Standards
- Eircodes/Postcodes
- Irish Water
- Primary On-line Database
- Individual Health identifiers/Health Identifiers Act
- Child Protection Issues
- Sepa Compliance
- Irish Genealogy website
- Smart Metering

We also advised on compliance with data protection policies within organisations, for instance how to use and store CCTV in a compliant manner. We are often consulted on areas such as transfer of medical records, transfers abroad, direct marketing, use of PPSN and use of medical data for research. During 2014 we dealt with over 1000 queries on subjects such as these from private and public sector organisations.

Binding Corporate Rules Reviews
Binding Corporate Rules are internal rules adopted by multinational groups of companies. These rules define the global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. Therefore BCRs ensure that all transfers made within a group benefit from an adequate level of protection. This is an alternative to the company having to sign standard contractual clauses each time it needs to transfer data to a member of its group. Once approved under the EU cooperation procedure, BCRs provide a sufficient level of protection to companies to get authorisation of transfers by national data protection authorities. It should be noted that the BCRs do not provide a basis for transfers made outside of the group.

In 2014 the Office was involved in co-reviewing the following BCRs, which have since been approved:

- First Data (Processor BCR - UK lead reviewer)
- Linkbynet (Processor BCR - France lead reviewer)
- TMF (Controller and Processor BCR's – Netherlands lead reviewer)

This Office is currently acting as the lead reviewer in two further BCRs, and in one other co-review.

Codes of Practice
Since 2008, when the Department of Finance produced a **Guidance Note on Protecting the Confidentiality of Personal Data** (http://www.ict.gov.ie/docs/Data_Protection_Guidelines.pdf), all government departments, offices and bodies have been encouraged to prepare a Code of Practice for their handling of personal data to be approved by the Data Protection Commissioner. The Commissioner would welcome more public-sector organisations approaching her Office with their draft Codes as a means of assisting them in improving their personal-data-handling practices.

The Commissioner is pleased to report that during the course of 2014, two data-protection Codes of Practice were approved under Section 13 of the Data Protection Acts. These Codes of Practice were approved for the Probation Service and the Department of Health. These approved Codes will provide a clear framework for these organisations when processing personal data in accordance with the Data Protection Acts. It is expected that these Codes will help customers to understand how their personal data is used and what standards they should expect in this regard.

Both of these organisations have worked closely with the Office to develop these Codes and the objectives have been achieved as the approved Codes provide a comprehensive guide to the Probation Service and the Department of Health regarding their responsibilities when it comes to protecting personal information.

The Commissioner would like to thank both of these organisations for adopting such a progressive attitude towards the benefits that can be derived from a Code of Practice on the use of personal data.

TYPICAL ENGAGEMENTS WITH TECH MULTI-NATIONALS

We undertake a significant amount of work with multinational technology companies with a headquarters or significant presences in Ireland. These are generally large-scale technology companies that offer web-based services. Often, the Irish Data Protection Commissioner is effectively the "lead" regulator for these companies regarding their activities in the European Union, under the European Union framework and by virtue of their European headquarters being located in Ireland. In 2014, we engaged with such companies on

numerous occasions in relation to existing products and services, proposed products and services, and other matters. In common with many regulators around the world, it is not possible to publicly disclose details of our engagement with these organisations, as this could negatively impact on the frankness of those conversations and therefore make effective regulation more difficult. However, the examples outlined below reflect our work with multinational technology companies, which is a significant element of our annual activity.

- Continuing engagement with Facebook Ireland prior to the introduction of new features, alterations to existing features, privacy settings and controls for individuals, advertising functions, and the recent launch of its new "Terms and Conditions" in January 2015. This included legal and technical examinations of the "user facing" elements of Facebook's offering, and the organisational and technical processing that goes on behind the scenes. In addition, a substantial on-site review of audit recommendations took place in mid-2014.

- Examination of a proposal from Apple to roll out a mobile mapping product, a legal and technical analysis of the proposal, and recommendations provided to the company on data-protection matters related to both Irish and possible other EU jurisdictions. All recommendations have been taken on board.

- Regarding our audit of LinkedIn, regular meetings and correspondence with LinkedIn to ensure the final privacy baseline of its service was detailed and addressed in that audit report. This involved lengthy engagement and evaluation on the progress of LinkedIn's actions based on the audit recommendations. Further updates to the LinkedIn service have also been discussed and work continues on refining the engagement process.

- Continuing updates from Microsoft on issues and clarifications relating to terms, agreements and establishment of certain services.

- Correspondence, site visits and examination of the Binding Corporate Rules and supporting organisational and technical measures for a number of cloud-based data processors now established in Ireland in the B2B sector.

- Consultative meetings with a number of international organisations seeking to establish in Ireland in relation to Internet of Things home devices, security and health data services in the cloud.

- Preparatory meetings, documentation submissions and reviews from a number of international organisations in Ireland ahead of possible audits or investigations.

- Meetings and correspondence with a number of international internet search organisations in Ireland in respect of the handling of the so-called "right to be forgotten" requirement.

GLOBAL PRIVACY SWEEP – MOBILE AND APPS

In May 2014, 26 privacy enforcement authorities, including Ireland, participated in the second Global Privacy Enforcement Network Privacy Sweep. The theme of the sweep – **Mobile Privacy** – was chosen because many privacy enforcement authorities had identified mobile apps as a key area of focus in light of the privacy implications for consumers.

In total, 1,211 apps were examined. They included a mix of Apple and Android apps, free and paid apps as well as public-sector and private-sector apps that ranged from games and health/fitness apps to news and banking apps.

In Ireland's case, the sweep involved the examination of 20 apps drawn from across various sectors, including transport, retail, media, banking, entertainment and government.

The most striking finding based on the results of the Irish sweep was that the team found that in 55% of cases examined, the privacy information provided by the apps only partially explained the collection, use and disclosure of personal information, with questions remaining with regard to some of the permissions requested. In terms of best practice, the sweep team examined two apps that related to personal finance – Ulster Bank and Tralee Credit Union – and found that both scored highly on how the app explains how it collects, uses and discloses the associated personal data. At the other end of the scale, the team found that three of the apps examined failed to provide adequate information to the customer, while one provided no privacy information whatsoever.

Going forward, the Office intends to examine the issues highlighted by the sweep in the context of our programme of audits in a similar way to how we included an examination of "cookies" information on the websites of entities we have audited since 2013.

In addition, and in line with our overall complaints function, we will examine any complaints made to us by members of the public in relation to data protection and mobile apps.

Finally, in terms of awareness, in 2014 we provided a series of presentations on cyber awareness to second-level students, which included questions aimed at 12–18 year olds, challenging them to consider, prior to the downloading of such apps, what personal data apps are seeking.

EUROPEAN UNION

New EU Data Protection Laws
The European Commission proposals for a new General Data Protection framework, which were published in 2012, continued to be the subject of much discussion in 2014. The European Parliament Committee (LIBE) had approved its text in October 2013 and awaits the Council of Ministers' text, which was still under discussion at the end of 2014. It is expected that the Council will agree its position in June 2015 and will then commence trialogue negotiations with the European Parliament and the European Commission.

Article 29 Working Party
In 2014, the Commissioner or the Deputy Commissioner attended all plenary meetings of the Article 29 Working Party, which acts as an advisor to the European Commission on data-protection issues. It also promotes a uniform application of EU data-protection law throughout the European Economic Area. During 2014 it exchanged ideas on many operational and policy issues.

Article 29 Subgroups
During 2014, members of staff of the Office of the Data Protection Commissioner attended the regular meetings of the Article 29 Technology Subgroup. Our participation in this panel is key to our commitment to consistency in policy and enforcement at a European level for technology issues. The topics covered in these meetings are wide and varied but have resulted this past year in cooperation on opinions regarding matters such as effective anonymity, the Internet of Things, device fingerprinting, big data, the Google Privacy Policy taskforce and cookie usage across Europe.

Other subgroups have been active in the areas of contract model clauses, national security, legitimate interests, risk approaches to data protection and binding corporate rules. Ireland's active role in these groups and opinions means that we can share expertise and knowledge with colleagues in Europe on a broad range of topics, while also discussing approaches to enforcement, and understanding the differences that sometimes occur in national implementations of the EU Data Protection Directive.

Joint Supervisory Bodies
During 2014, members of staff attended meetings of the Joint Supervisory bodies of JSB Europol and JSA Customs. These groups were established to monitor the processing of personal data in large pan-European databases operated by Europol and European customs authorities. The Office also participated in a week-long audit of Europol systems conducted at Europol's HQ in The Hague.

The Court of Justice of the European Union (CJEU)

Data Retention Directive Case
The Data Retention Directive (2006/24/EC) requires telecoms and other electronic communications businesses to retain identifying details of telephone calls and emails such as traffic and location data, to help the police detect and investigate serious crimes. The content of those communications is excluded.

In April 2014, the CJEU found that the Data Retention Directive was invalid on the grounds that the EU legislators had exceeded the limits of proportionality in forging the Directive. It held that the Directive entailed serious interference with the rights to privacy and personal data protection of individuals provided for by the Charter of Fundamental Rights. The Directive also failed to establish limits on access by competent national authorities, such as prior review by judicial or independent administrative authority.

The effect of the judgment is that any EU member state that has transposed the Directive into national law has to ensure that such law is in compliance with the judgment. A number of EU states have either scrapped or amended their legislation as a result of the judgment. This Office understands that the Department of Justice and Equality is considering any implications of the CJEU decision.

Google Spain Case
In May 2014, the CJEU issued its judgment in the case of Google Spain v AEPD and Mario Costeja (Case C-131/12). (It is commonly known as the Google Spain case or the "right to be forgotten" case).The Court held that an internet search engine is responsible for the processing that it carries out of personal information appearing on web pages published by third parties.

Due to the ruling, the internet search engine is obliged to consider requests from individuals to remove links to freely accessible web pages that result from a search of their name. The Court set out a number of grounds for removal. If the search engine rejects the request from the individual then s/he can request their local data-protection authority (DPA) to consider the case. If the DPA finds in favour of the individual then the search engine may be ordered to remove the links from search results. In order to have a consistent process in place to consider requests from individuals, the Article 29 Working Party drafted a set of Guidelines to assist DPAs.

The ruling not only led to the requirement for search engines to delist results concerning individuals in certain cases, but also had a potential impact on jurisdictional matters where establishments have offices or legal entities in more than one European country.

CCTV Household Exemption case
In December 2014, the CJEU handed down its judgment in the case of Rynes (Case C-212/13). It related to the processing of personal data in the operation of a domestic CCTV system that was installed to protect the property, health and life of the occupants; however, the system also monitored a public space.

The outcome of the case has significant implications on the application of Article 3(2) of the Data Protection Directive (95/46/EC). Under Article 3(2), the Directive did not apply to the processing of personal data done by a person in the course of personal or household activity, commonly known as the "household exemption". However, the CCTV in this case was capturing footage of the entrance to a neighbouring property

and the public highway. The footage was used in a criminal case.

The Court held that household exemption should be narrowly construed and it only applies to processing in the course of purely personal or household activity. It found that public surveillance by a private household system fell outside Article 3(2). This means that domestic use of CCTV that captures public roads, walkways etcetera could be construed as being a data-controller operation and subject to access requests by members of the public on the data captured by the CCTV. Therefore, the decision has implications for the application of the household exemption as provided for in Section 4 of the Data Protection Acts 1988 and 2003.

The Office of the Data Protection Commissioner will take into account the CJEU judgment when considering issues arising in relation to the household exemption.

OTHER INTERNATIONAL ACTIVITIES

The office was represented at the 35th International Conference of Data Protection and Privacy Commissioners, which was held in Mauritius in September 2014. The main theme of the conference was the Internet of Things.

The office also followed the useful work done by the OECD, particularly as regards cross-border enforcement of data protection.

Beyond the EU level, we actively continue to participate in technology-related matters in the International Working Group on Data Protection in Telecommunications (IWGDPT) and in the newly formed Internet Privacy Engineering Network (IPEN).

The office was also a contributor to matters in the Global Privacy Enforcement Network (GPEN), where cooperation and knowledge can be shared globally with dat-protection authorities outside of Europe – a key issue considering that many North American or other multinationals established in Ireland are representatives for all users outside of the USA.

During 2014, the Office continued its involvement with the International Association of Privacy Professionals (IAPP), including attendance at its Brussels summit in November 2014.

APPENDICES

LIST OF ORGANISATIONS AUDITED OR INSPECTED IN 2014

Overall, the inspection teams found that there was a reasonably high awareness of, and compliance with, data-protection principles in the organisations that were inspected. Notwithstanding this, the majority of organisations had areas where immediate remedial action was necessary. It was noted with satisfaction that the majority of the data controllers audited have demonstrated a willingness to put procedures in place to ensure they are meeting their data-protection responsibilities in full. The Commissioner would like to thank all of the organisations audited and inspected throughout the year for their cooperation.

- Irish Farmers Association
- Lifestyles Online Ireland Ltd t/a Data Xcel
- Abtran
- Athlone Money Advice & Budgeting Service (MABS)
- Kildare Motor Tax Office
- Thurles Citizens Information Service
- Therapie
- Whitewater Shopping Centre (CCTV)
- Garwyn Liability Adjustors
- Jervis Shopping Centre (CCTV)
- National Driver Licence Service
- "Your Service Your Say" (HSE)
- Liability Claims Appraisers Ltd
- Citizens Information Board
- Parkbytext
- Pageboy (related to Parkbytext audit)
- Unislim
- MCK Rentals Ltd t/a MCK Investigations Ltd
- Mara & Young Accountants
- Byrne O'Byrne Associates
- Chartered Accountants Ireland
- UCD Records Office
- M & F Finance Ltd
- Lucan District Credit Union
- Positive Moves, Rialto
- Limerick CIE Employers Credit Union
- St Canices Credit Union
- Carrick on Shannon & District Credit Union
- Glancys Supervalu Carrick on Shannon
- Ballynacargy Community Childcare Services
- Mullingar Credit Union
- Bray Credit Union
- Toplook, Dublin
- Thurles Credit Union
- Soundstore, Cork
- Catoca t/a Emo Tea Rooms
- EGIS (Port Tunnel Toll Booths)
- National Gallery of Ireland

CASE STUDIES

Case Study 1:
Prosecutions: Private Investigators

This Office initiated prosecutions in the private investigator/tracing-agent sector for the first time in 2014. These prosecutions arose from a detailed investigation that commenced in the summer of 2013. Arising from audits carried out in a number of credit unions at that time, the Office became concerned about the methods employed by some private investigators hired by credit unions to trace the current addresses of members who had defaulted on their loans. The Office launched a major investigation to identify the sources from which the private investigators had obtained the current address data. This investigation involved a wide range of public bodies and private companies. As a result of our findings, the Office established that personal data on databases kept by the Department of Social Protection, the Primary Care Reimbursement Service of the Health Service Executive, An Garda Síochána and the Electricity Supply Board had been accessed unlawfully and the information was disclosed thereafter to credit unions. Details of the prosecutions that ensued are as follows:

M.C.K. Rentals Limited and its Directors

M.C.K. Rentals Limited (trading as M.C.K. Investigations) was charged with 23 counts of breaches of Section 22 of the Data Protection Acts 1988 and 2003 for obtaining access to personal data without the prior authority of the data controller by whom the data is kept, and disclosing the data to another person. The personal data was kept by the Department of Social Protection (7 cases) and by the Primary Care Reimbursement Service of the Health Service Executive (16 cases). In all cases, the personal data was disclosed to various credit unions in the state.

The two directors of M.C.K. Rentals Limited, Ms Margaret Stuart and Ms Wendy Martin, were separately charged with 23 counts of breaches of Section 29 of the Data Protection Acts 1988 and 2003 for their part in the offences committed by the company. This Section provides for the prosecution of company directors where an offence by a company is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, the company directors or other officers.

At Bray District Court on 6 October 2014, M.C.K. Rentals Limited pleaded guilty to five sample charges for offences under Section 22 of the Data Protection Acts 1988 and 2003. The Court convicted the company in respect of each of the five charges and it imposed a fine of €1,500 per offence. Company Secretary and Director Ms Margaret Stuart pleaded guilty to one sample charge for an offence under Section 29 of the Data Protection Acts 1988 and 2003. The Court convicted Ms Stewart in respect of that offence and imposed a fine of €1,500. Company Director Ms Wendy Martin pleaded guilty to one sample charge for an offence under Section 29 of the Data Protection Acts 1988 and 2003. The Court convicted Ms Martin in respect of that offence and it imposed a fine of €1,500.

This was the first occasion on which company directors were prosecuted by the Data Protection Commissioner for their part in the commission of data-protection offences by their company, and the proceedings in this case send out a strong warning to directors and other officers of bodies corporate that they may be proceeded against and punished in a court of law for criminal offences committed by the body corporate.

The investigation of this company uncovered wholesale and widespread "blagging" techniques used by the offenders, and this was the first prosecution by the Data Protection Commissioner of offenders engaged in such practices. The findings of the investigation carried out in this case expose the constant threat to the security of personal data that is in the hands of large data controllers and the vigilance that is required by front-line staff at all times to prevent unlawful soliciting of personal data, in particular by means of telephone contact, by unscrupulous agents. Data controllers across the state should regularly review their data-protection procedures to maximise the effectiveness of their security protocols in order to counter such criminal activity. They must ensure that all staff, and particularly those at the front line who handle telephone calls, are fully trained in the security protocols in order to be able to recognise and deal with the threat of information blagging or pretext calling if it arises.

Michael J. Gaynor

Michael J. Gaynor (trading as MJG Investigations) was charged with 72 counts of breaches of the Data Protection Acts 1988 and 2003. Twelve charges related to breaches of Section 22 of the Data Protection Acts for obtaining access to personal data without the prior authority of the data controller by whom the data is kept, and disclosing the data to another person. The personal data was kept by the Electricity Supply Board (9 cases) and by An Garda Síochána (3 cases). In all cases, the personal data was disclosed to various credit unions in the state. A further 60 charges related to breaches of Section 16(2) of the Data Protection Acts in respect of the processing of personal data of a number of individuals in circumstances where no record was recorded in respect of the accused in the public register maintained by the Data Protection Commissioner. Mr Gaynor is a former member of An Garda Síochána.

On 25 November 2014, at Dublin Metropolitan District Court, Michael J. Gaynor was convicted on two charges for offences under Section 22 of the Data Protection Acts 1988 and 2003. The Court imposed a fine of €2,500 in each of these two charges. Separately the defendant pleaded guilty to 69 charges (60 of which related to breaches of Section 16(2)) and these were taken into consideration in the sentence imposed.

This was the first prosecution to be completed by the Data Protection Commissioner of a data processor for processing personal data without having registered as a data processor on the public register of the Office of the Data Protection Commissioner. The investigation in this case uncovered access by the defendant

to customer data held on databases held by the Electricity Supply Board. To access the personal data, the defendant used a staff contact in the Electricity Supply Board, which he had established during his previous Garda career.

These prosecutions send a strong message to private investigators and tracing agents to comply fully with data-protection legislation in the conduct of their business, and that if they fail to do so they will be pursued and prosecuted for offending behaviour. They also serve to remind all companies and businesses who hire private investigators or tracing agents that they have onerous responsibilities under the Data Protection Acts to ensure that all tracing or other work carried out on their behalf by private investigators or tracing agents is done lawfully. Specifically, in this regard, those operating in the credit union, banking, financial services, legal and insurance sectors should review their engagement of private investigators and tracing agents to ensure they have fully safeguarded all personal data against unlawful forms of data processing.

These investigations uncovered serious issues in relation to the hiring of private investigators or tracing agents by credit unions, particularly in respect of a lack of awareness on their part of how the private investigators were tracing members and, in some cases, in relation to the disclosure of PPS numbers by credit unions to private investigators. This Office has pursued all of these issues with the credit unions concerned and with their representative bodies in recent months. In addition, we have undertaken a range of follow-up work with the Department of Social Protection, the Health Service Executive, An Garda Síochána and the Electricity Supply Board on the implications of the data-security breaches that occurred in their organisations and on the measures required to deal with those breaches and to prevent a recurrence. This Office welcomes the fact that the Private Security Authority has proposed the introduction of regulation of private investigators.

Case Study 2: Prosecutions: Marketing Offences

Pure Telecom Limited

We received a complaint in March 2013 from an individual who received two marketing phone calls from Pure Telecom Limited on his landline telephone. The individual's telephone number was listed on the National Directory Database opt-out register. It is an offence to make a marketing call to a telephone number listed on that register.

Pure Telecom Limited informed our investigators that it used the services of a third-party representative to make the marketing calls and it explained that the agent sourced the individual's number themselves rather than using marketing data provided by Pure Telecom Limited. The company admitted that the third-party agent did not have consent to contact the complainant for marketing purposes.

At Dublin District Court on 3 February 2014, Pure Telecom Limited pleaded guilty to two charges concerning breaches of Regulation 13 (5)(b) of S.I. 336 of 2011 relating to two marketing phone calls to a phone number listed on the opt-out register. The Court imposed a conviction in respect of both charges and a fine of €500. It further ordered payment of the prosecution costs of the Data Protection Commissioner. The hearing was informed that the defendant had a previous conviction from 2010 for a similar offence.

Next Retail Limited

In February 2013, this Office received a complaint from an individual who received a number of unsolicited marketing emails from Next Retail Limited after she requested the company not to send her any more such emails. The complainant claimed to have unsubscribed firstly by using the unsubscribe link that was provided in a marketing email sent by the company and, following this, in four separate emails to the company requesting not to be contacted with marketing emails again.

Next Retail Limited informed our investigators that as it no longer used the services of the company that it had engaged to process unsubscriptions it was unable to explain what happened to the first unsubscribe request. With regard to the emails containing unsubscribe requests, the company confirmed that they did reach its complaints inbox but it was unable to trace where the emails went afterwards.

At Dublin District Court on 3 February 2014, Next Retail Limited pleaded guilty to two charges concerning breaches of Regulation 13(1) of S.I. 336 of 2011 relating to the sending of two unsolicited marketing emails without consent. The Court imposed a conviction in respect of one charge, with the second charge taken into consideration. A fine of €100 was imposed. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

Next Retail Limited subsequently appealed the severity of the sentence. On 19 March 2014, the Circuit Court affirmed the conviction and penalty previously imposed by the District Court and it noted the appellant's intention to discharge the Data Protection Commissioner's reasonable costs for the appeal.

Airtricity Limited

In May 2013, this Office received a complaint against Airtricity Limited from a person who received an unsolicited marketing phone call on his landline telephone, which was listed on the National Directory Database opt-out register. The complainant informed us that the purpose of the marketing call was to encourage him to switch energy supplier to Airtricity.

In response to our investigation, Airtricity admitted that the phone call had been made by a third-party contractor acting on its behalf. It explained that the error occurred when an old PC, on which the 2009 phone book was installed, was re-commissioned by the contractor. A spreadsheet containing the complainant's phone number was still on the old PC and this led to the number being dialled in error.

At Dublin District Court on 3 February 2014, Airtricity Limited pleaded guilty to one charge concerning a breach of Regulation

13(5)(b) of S.I. 336 of 2011 relating to one marketing phone call to a phone number listed on the opt-out register. The Court imposed a conviction in respect of the charge and a fine of €75. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner.

The Carphone Warehouse Limited

In March 2013, we received a complaint from a customer of The Carphone Warehouse Limited after he received marketing text messages from the company despite having ticked the marketing opt-out box when he had previously made a purchase in one of its stores. The company informed our investigators that a systems error resulted in the customer being incorrectly included in its marketing list.

In April 2013, we received a complaint from another customer of The Carphone Warehouse Limited who received regular offers by text message from the company even though he had called the company on at least three occasions, asking that it stop. The company told our investigators that its system temporarily did not recognise the customer's preference not to receive marketing due to an internal issue within the electronic filter process and this resulted in the customer's phone number being accidentally selected for marketing campaigns.

At Dublin District Court on 3 March 2014, The Carphone Warehouse Limited entered a guilty plea in respect of five charges concerning breaches of Regulations 13(1) and 13(4) of S.I. 336 of 2011. The court imposed convictions in respect of four charges, with the fifth charge taken into consideration. It imposed fines of €1,500 in respect of each conviction. The defendant agreed to cover the prosecution costs of the Data Protection Commissioner. The hearing was informed that the defendant had two previous convictions from 2012 in relation to the sending of unsolicited marketing emails.

Valterous Limited (trading as Therapie Clinic and/or Therapie)

A former customer of Valterous Limited (trading as Therapie Clinic and/or Therapie) complained to this Office in June 2013 after receiving an unsolicited marketing text message despite having opted out of receiving such communications over three months earlier. Therapie explained to our investigators that the complainant's contact details were on systems in two branches and that when the opt-out request was made the company removed their details from one database and did not realise they were also on another one, thus leading to a further unsolicited text message being sent to the same contact number.

In July 2013, we received a complaint from another former customer of Therapie who had received marketing text messages on several occasions. The complainant informed us that she sent a text message to opt out but the company continued to send her further marketing text messages. Our investigation found no evidence that Therapie had obtained consent at any time for the sending of marketing text messages to this individual. In relation to the sending of text messages after the former customer had opted out, Therapie explained that the individual should have texted the word "STOP" rather than the word "OPTOUT" at the time of attempting to opt out of the marketing database. We did not accept this as a valid excuse as the opt-out instruction on the marketing text message sent to the individual read "OptOut:086.....".

At Dublin District Court on 3 March 2014, Valterous Limited (trading as Therapie Clinic and/or Therapie) pleaded guilty in relation to three charges concerning breaches of Regulation 13(1) of S.I. 336 of 2011 concerning the sending of unsolicited marketing text messages without consent. The Court imposed convictions in respect of two charges, with the third charge taken into consideration. It imposed fines of €1,500 in respect of each conviction. The defendant agreed to pay the prosecution costs of the Data Protection Commissioner. The Court was told that in 2012 Therapie Laser Clinics Limited (trading as Therapie Clinic and/or Therapie) was convicted for two offences in relation to the sending of unsolicited marketing text messages.

Case Study 3: Excessive Data Collection by An Post

This Office received two complaints from members of the public concerning new requirements that were introduced in November 2013 by An Post in relation to direct-debit applications for payment of TV licence fees. A mandatory requirement was introduced to provide a recent bank statement with the direct-debit application and mandate form. An Post's TV licence website explained that a copy of a bank statement was required to verify the bank-account details provided by the licensee for payment of their TV licence fee. It went on to state that the bank statement must show the BIC, IBAN and the full name and address of the bank-account holder. The complainants argued that requesting a copy of confidential financial information that appears on bank statements was excessive.

We investigated these complaints with An Post. By way of background, An Post explained that the new SEPA regulations impose significant new obligations on direct-debit originators such as An Post with the TV Licence Direct Debit Scheme. It said that the commercial risk attached to accepting direct debits is now the sole responsibility of An Post and therefore An Post has to verify the direct-debit details supplied by the customer. It stated that An Post does not have proof that the bank-account details exist, are accurate or that the account is owned by the person stated on the mandate. Accordingly, it developed its new bank-detail verification process to check the mandate details supplied, and in that new process it seeks extra documentation to verify that the bank-account details supplied by the applicant are accurate, complete and up to date. It also pointed out that it cannot process a direct-debit application without having valid BIC and IBAN numbers in respect of the account on which the direct debit is drawn. An Post indicated that, further to our correspondence, it had decided that customers who choose direct-debit payment are no longer required to submit details of their bank balances.

We considered the matter further and we advised An Post that applicants should either be allowed to submit a copy of only the portion of the bank statement containing the name, address, BIC and IBAN numbers or they should be allowed to blacken out all of the transaction information on any copies supplied. An Post agreed to implement our advice. It amended its TV licence direct-debit application form to include the following text: "You should ensure that financial transactions on your bank statement are fully masked or removed before you attach it to your application. All bank statements are destroyed once the first successful payment has gone through." An Post also amended its website to reflect this change and to clarify that it does not require the balance on the bank statement to be shown. We were satisfied with the changes implemented by An Post and with the manner in which it dealt with the matter expeditiously once we had drawn it to its attention.

Organisations that seek copies of bank statements for purposes such as proof of current address, as a verifier of identify or other similar issues should bear in mind that such documents contain a range of financial information that is private to the individual to whom it relates. As a general rule, individuals must be permitted to blacken out or otherwise mask those financial details and transactions as they are irrelevant for the purposes of address verification, etc. This case study should serve as a reminder to organisations to consider all the implications and the potential to collect an excessive amount of personal data in circumstances where they seek copies of bank statements from customers or clients.

Case Study 4: Disclosure of Employee Salary Details by the HSE

An employee of the Health Service Executive (HSE) complained in March 2014 concerning the alleged disclosure on two occasions of his salary details to his ex-wife. He informed us in his complaint that the matter came to his attention when his ex-wife went to court in the summer of 2013 in relation to maintenance issues, and in court she provided exact details from his payslips. In December of the same year, his ex-wife went back to court for a review of maintenance and on that occasion she produced a copy of his P60 along with his salary details for the previous four months.

We commenced an investigation of the matter by writing to the HSE. In response, the HSE accepted that on two separate occasions, in May 2013 and in November 2013, personal data relating to its employee was disclosed to a third party without his consent. It acknowledged that there was no legal basis for the disclosure of the personal data. It stated that it established who, within the HSE, made the first disclosure but it was not possible to establish who made the second disclosure. It explained that its payroll department had received a number of court orders directing the HSE to make maintenance payments to its employee's ex-wife. It stated that numerous queries were raised by a firm of accountants and tax professionals called Accountax on behalf of its employee's ex-wife. Those queries sought clarifications with regards to the payments made. It went on to state that, in relation to the first breach, a specific request was made seeking a copy of its employee's most recent payslip showing the maintenance deductions from January 2013 to date. The HSE admitted that the requests for constant updates regarding maintenance payments ultimately resulted in the unauthorised disclosure of its employee's personal data. The HSE accepted that in hindsight the only data that should have been released by its payroll department to its employee's ex-wife (or to a person acting on her behalf) was a summary of payments made that related to the court orders.

We informed the HSE that we considered that the Data Protection Acts were breached when the personal data of its employee was disclosed to a third party without his consent. The HSE indicated that it wished to pursue an amicable resolution to the complaint and, to this end, it enclosed a letter of apology for the complainant. The data subject considered the letter of apology and he decided that he did not wish to accept it, opting instead to seek a formal decision of the Data Protection Commissioner on his complaint.

A decision of the Data Protection Commissioner was issued in August 2014. In his decision, the Commissioner formed the opinion that the HSE contravened Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003 on two occasions by the further processing of the complainant's personal data in a manner incompatible with the purpose for which it had been obtained. These contraventions occurred in May 2013 and in November 2013 when the HSE disclosed his personal information to a third party. Section 2(1)(c)(ii) of the Data Protection Acts 1988 and 2003 provides that data shall not be further processed in a manner incompatible with the purpose for which it was obtained. In this case, the HSE acknowledged that on two separate occasions the personal data was disclosed to a third party without the consent or knowledge of the data subject. Such disclosures constitute further processing of personal data.

Case Study 5: Excessive Data Collection by a Letting Agency

In July 2014, a prospective tenant complained about the collection of bank details, PPS numbers and copies of utility bills by a letting agency when applying to rent a property. The complainant stated that this information was in addition to the usual material, such as previous landlord's reference, which one would expect to submit at application stage. She stated that she believed that if she did not supply all of the sought data up-front, her application would not be seriously considered by the letting agency. The complainant said that the practice of collecting such a broad range of personal data forces prospective tenants who are desperate to rent a property to submit this personal information at application stage even though they do not know if their application will be successful. She pointed out that the majority of applications are unsuccessful given the high demand for a limited supply of available rental properties in the Dublin area.

We commenced an investigation of the matter with the letting agency concerned, seeking an explanation for the collection of such a broad range of personal data at application stage. In response, the letting agency said that it requested PPS numbers from applicants because this verifies that they are entitled to work in the state, and that bank details are required to show that a tenant has a bank account because they would be ineligible if they were not able to pay rent through a bank account. We told the letting agency that we could not see any basis for collecting bank details, PPS numbers or copies of utility bills at application or property-viewing stage and we urged it to cease the practice immediately. We questioned the letting agency further about using the PPS number to verify the applicant's work status. It replied to the effect that the main reason it requests PPS numbers is that it is required for the Private Residential Tenancies Board (PRTB) registration form and it said that it cannot register a tenant without it. It went on to say that it is only an added assurance that the applicant is working and it stated that it does not verify the PPS number.

We accepted that personal data concerning bank details, PPS numbers and utility bills could be requested once the applicant had been accepted as a tenant. In October 2014, the letting agency confirmed, following our investigation, that it had ceased the requesting of this personal data prior to the property being let and it undertook that it would only request this information once the tenant had been accepted. The complainant informed us that she was very satisfied with the outcome of her complaint.

This case study is a classic example of the temptation of some data controllers to collect a whole range of personal data in case they might need it in the future. In this case, the letting agency collected a significant amount of personal data from every applicant who expressed an interest in renting a property even though, at the end of the process, only one applicant could be accepted as the new tenant and it was only in the case of that successful applicant that the full range of personal data was required. Section 2(1)(c)(iii) places an obligation on data controllers to ensure that personal data which they process is adequate, relevant and not excessive in relation to the purpose or purposes for which it is collected or are further processed. Data controllers must be mindful of this requirement and abide by it despite the temptation for convenience or other reasons to embark on an unnecessary broad data collection exercise.

Case Study 6: Disclosure of Financial Information by a Credit Union

A member of a credit union complained in 2013 in relation to the alleged disclosure of his loan and savings information by the credit union to his daughter. By way of background, the complainant explained that he was a guarantor on a credit union loan to his daughter. He received a letter from the credit union to inform him of difficulties that his daughter was experiencing with her loan. The purpose of the letter was to call on him, as the loan guarantor, to pay the balance of monthly repayments. He outlined that the letter was addressed to him and that it contained his membership number along with his savings and loan details, including balance outstanding. Soon afterwards, his daughter called to his house with a copy of the same letter as the credit union had also sent it to her. The complainant said that he considered this disclosure of his financial information to be a gross violation of his privacy.

We investigated the matter with the credit union concerned. It explained that the error that led to the disclosure occurred when the letter to the guarantor was issued under the guarantor's membership number and not under the membership number of his daughter, whose loan it referred to. It explained that the computer system automatically brings across the account details of the membership number keyed in. The credit union admitted that a member of its credit-control staff inadvertently typed the letter under the guarantor's membership number and, as a result, his account details were printed on the letter.

The credit union proposed that, as a means of trying to reach an amicable resolution of the complaint, it would issue a letter of apology to the guarantor. It also carried out staff training in regard to issuing letters to members, in particular letters to guarantors, and it re-circulated its data-protection policy to all staff. The complainant considered the offer and rejected it. He sought a formal decision of the Data Protection Commissioner on his complaint.

In April 2014, a decision issued to the complainant. In his decision, the Commissioner formed the opinion, following the investigation of the complaint, that the credit union contravened Section 2(1)(d) of the Data Protection Acts by providing details of the complainant's membership account to a third party by means of a letter that was copied to the third party. Section 2(1)(d) obliges data controllers, among other things, to take appropriate security measures against unauthorised disclosure of personal data.

This case highlights the serious consequences for the complainant concerned arising from what appeared to be an innocuous error on the part of the staff member typing a letter for the complainant on his own account rather than on the account of his daughter, to whom the subject matter of the letter related. It serves as a reminder to data controllers generally to keep data-protection awareness to the forefront, with regular staff training for those whose work involves any form of data processing.

Case Study 7: Complaint of Disclosure by Permanent TSB Not Upheld

A complaint from a customer of Permanent TSB alleged that the bank had violated the Data Protection Acts by discussing their accounts and personal details with a third party, the complainant's tenant, thereby causing financial loss and stress.

We investigated the allegation with Permanent TSB. In response, the bank informed us that it had made no contact with residents in the properties concerned to discuss the mortgage account details of the complainant concerned. It further stated that all telephone calls received from the

tenant concerned had been listened to and at no time did any staff member discuss the details of the mortgage account with her. As part of our investigation we sought a copy of the recordings of phone calls that took place between Permanent TSB and the tenant. We listened to the call recordings and we were satisfied that no personal data relating to the complainant was passed to the tenant during the phone calls with Permanent TSB. Instead, the tenant was repeatedly told that Permanent TSB could not discuss anything with her without the written authority of the account holder. In one instance, the tenant offered to give her contact number to Permanent TSB but she was informed that it was not required as Permanent TSB would not be contacting her. This Office's investigation found no evidence that Permanent TSB disclosed any personal data relating to the complainant to the third party concerned.

In a separate aspect to the same complaint, it was alleged by the complainant that Permanent TSB had sent correspondence to a previous residential address after it had been notified of a change of address. The complainant supplied us with a copy of a letter sent by them in August 2011 notifying the bank of the new address for correspondence and we were also supplied with copies of letters sent by Permanent TSB to the previous address after that date. In response to our investigation of this matter, Permanent TSB confirmed that it had received the August 2011 letter, which notified it of the new address, but it could offer no explanation as to why its systems had not been updated at that time to reflect this. It informed us that it was not until it received a further letter in January 2012 that the system was updated. To assist with trying to resolve the complaint, the bank offered a goodwill gesture as an acknowledgement of the delay encountered and of any stress the delay may have caused, but this was rejected by the complainant.

The complainant sought a formal decision on the complaint. With regard to the failure to update the contact address, having been requested to do so in August 2011, the Commissioner formed the opinion that Permanent TSB contravened Section 2(1(b) of the Data Protection Acts. This section obliges data controllers to comply with the requirement to keep personal data accurate and up to date.

With regard to the allegation of disclosure of the complainant's personal data to a tenant, the Commissioner was unable to form the opinion that a contravention of the Data Protection Acts occurred in this instance.

Case Study 8: Patient Denied Right of Access by SouthDoc

We received a complaint in June 2014 from a firm of solicitors whose client had made an access request in May 2014 to the Practice Manager at South West Doctors-On-Call Limited (trading as SouthDoc) seeking a copy of his medical notes. In response to the access request, SouthDoc replied to the solicitors, stating that they are advised to contact the patient's own GP, who holds a complete record for the patient. The solicitors wrote back to SouthDoc, pointing out that the access request was made to SouthDoc and that it was a separate request to any request their client may make to his own GP. The solicitors pointed out that SouthDoc was obliged to comply with the request. In submitting the complaint to this Office, the solicitors informed us that SouthDoc had not replied to their latest letter but had returned it to them unanswered.

We began an investigation by writing to SouthDoc. It responded by return post, indicating that the request for medical records had now been dealt with. Soon afterwards, the solicitors for the complainant supplied us with a copy of a letter they had received from SouthDoc stating that, further to the access request, the patient's records had been forwarded to his own GP. The solicitors pointed out that SouthDoc had not complied with the access request as it was their client who requested the records, and it was not sufficient for SouthDoc to give them to his GP. We wrote to SouthDoc again, seeking an explanation. A few days later we received from SouthDoc a copy of a letter that it had issued to the patient's solicitors, enclosing a copy of the patient's medical records. We then concluded our investigation.

There are a number of after-hours or on-call service providers such as SouthDoc in operation in Ireland, all of which provide an essential medical service for the general public. In doing so, these service providers collect and process both personal data and sensitive personal data (data relating to the physical or mental health of the attending patient). For the purposes of data protection, it is important that patients and service providers understand that when a patient attends one of those services, they provide their personal data to an organisation (data controller) that is entirely separate to their usual GP practice. Accordingly, the records created by the service provider in respect of the patient's attendance and treatment are new records in respect of which the service provider is the data controller. For that reason, the patient has a right to access those records directly from the service provider by making an access request for a copy of them. This right of access to the records of the service provider exists whether or not the service provider passes on details of the patient's attendance and treatment to the patient's GP. Furthermore, the service provider is obliged to supply a copy of the personal data directly to the requesting patient (or to the solicitor acting on his behalf, as in the above case) rather than to the patient's own GP. (Access to medical records is subject to the provisions of S.I. 82 of 1989, which prohibits the supply of data to a patient in response to an access request if that would cause harm to his or her physical or mental health.)

Case Study 9: Excessive Data Collection by the Department of Agriculture

An individual complained to this Office about new requirements introduced by the Department of Agriculture to produce bank-account details in relation to registering premises to comply with the Diseases of Animals Act 1966–2001. He explained that horse owners are required to register the premises in which horses are kept with the Register of Horse Premises and he said he had no difficulty with that requirement.

However, he objected to being asked to supply his bank-account details and he pointed out that there was no possibility of this information being needed by the Department as there were no schemes or grants that entitle horse owners to payment. He told us that he and his wife each own a horse and that both horses are kept purely for pleasure purposes. He said that he had expressed his concerns directly to the Department initially but the Department continued to insist that he submit bank details.

We sought an explanation from the Department of Agriculture. In its response, the Department referred to the government's drive towards e-commerce and the fact that government departments can no longer issue payable orders. It said that payments due by the Department can only be made by way of electronic fund transfer to a bank account. Accordingly, all clients of the Department in receipt of payments are asked to supply bank details as a prerequisite for entry onto the Department's Corporate Customer System. It said that as most of the Department's clients are in receipt of payments or could potentially receive payments, it was decided that all new clients (applicants), including those who exceptionally might not currently qualify for payments, would be asked for their bank-account details.

We referred the Department to the provisions of Section 2(1)(c)(iii) of the Data Protection Acts, which places a requirement on data controllers to ensure that personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is collected. We pointed out that the principle established by this provision required that personal data should be collected when required and not on the basis that it might be required at some future point. We received confirmation from the Department in February 2014 that the practice of seeking bank details in anticipation of possible future payments had ceased. We were informed that an information notice had been issued to staff, stating that customer bank details are required only where a customer will be in receipt of payments from the Department.

The complainant in this case raised a very valid complaint with this Office, having failed to resolve the matter directly with the Department himself. Insufficient thought appears to have been given at the outset to the concept of requiring bank details from every customer or potential customer of the Department – whether that information was needed or not. More disappointingly, however, was the fact that the Department did not review the situation and fix it after this individual drew the Department's attention to his circumstances and the circumstances of others who keep horses for pleasure purposes – pointing out that the Department would never need to use his bank-account details as he was not an applicant for a scheme or grant. In the end, it took the intervention of this Office to persuade the Department to cease seeking excessive personal data and to comply with the principle that data collection shall be adequate, relevant and not excessive.

Case Study 10: Personal Data Disclosed by County Council

In April 2014, we received a complaint from an individual who alleged that her private email address was disclosed to third parties without her permission by Dun Laoghaire Rathdown County Council. The complainant had made a submission to the county council in respect of a local area plan. She found out about the disclosure when one of the parties to whom her email address had been disclosed made an unsolicited contact with her using her email address. She indicated that she was worried as she did not know how many people were in possession of her private email address as a result of the disclosure.

We commenced an investigation by writing to Dun Laoghaire Rathdown County Council. In response, the county council by way of background explained that it supplies notices, agendas and minutes of its meetings to parliamentary representatives in accordance with Local Government Act 2001 (Section 237A) Regulations 2003.

It went on to state: "It has been the practice of this Authority heretofore to supply copies of all reports that issue with these agenda, as this is how the agenda issues to our councillors. In accordance with the Planning and Development Act 2000 [as amended], Section 20(3)(c)(ii), a Manager's Report for a Local Area Plan must list the persons who made submissions or observations. In all cases a list of submitters is prepared, for internal use and file, which includes necessary contact details, home address and email address. It is our standard practice, however, to remove the email addresses before circulation to councillors. The home addresses are left on as councillors wish to see who in their constituency made a submission. In this case we inadvertently included the email and home addresses with the list of submitters. This was an error on our part, and not standard practice. What has been placed on our website, however, is the list without the contact details. In order to prevent a recurrence of this, we have reminded all staff not to include the contact details of submitters in reports which are circulated to councillors or placed on the website. Additionally, although as mentioned above the list that went to councillors usually contained the submitter's address for the councillors' information, we will not include either home address or email address in any reports issuing to councillors. In addition to the above, and to further prevent the inadvertent release of personal information, the Council will cease the practice of issuing reports with the agenda which are supplied to parliamentary representatives."

The county council stated that it had issued a revised report, with all of the personal contact details removed, to all of the recipients and it asked that they delete the original version. The county council concluded by saying that in this case the information was disclosed accidentally and it said that it would endeavour to ensure that there will be no repeat of this incident by adhering to its standard procedure and by reminding all staff concerned of those procedures.

The complainant sought a formal decision on her complaint.

Section 2(1)(c)(ii) of the Data Protection Acts provides that personal data shall not be further processed in a manner incompatible with the purpose for which it was obtained. The data controller in this case, Dun Laoghaire Rathdown County Council, explained to our investigation that in accordance with the Planning and Development Act 2000, a County Manager's Report for a Local Area Plan must list the persons who made submissions or observations. The data controller further stated that in all cases a list of submitters is prepared for internal use, which includes contact details, home address and email address, and that it is its standard practice to remove the email addresses from this list before circulation to councillors. However, it was clear that in this particular instance the email addresses of the submitters was not removed from the circulation list. In making his decision, the Commissioner formed the opinion that Dun Laoghaire Rathdown County Council contravened Section 2(1)(c)(ii) of the Data Protection Acts. This contravention occurred by the further processing of the complainant's personal data in a manner incompatible with the purpose for which it had been obtained when her email address was disclosed by Dun Laoghaire Rathdown County Council via the circulation of a report to county councillors, TDs and senators in relation to a local area plan.

Case Study 11: Eircom Fails to Meet Statutory Timeframe for Processing Access Request

A staff member of Eircom submitted a complaint to this Office in relation to the alleged failure of Eircom to comply with an access request submitted by him to the company in September 2013. In his access request, he specifically requested a copy of a particular letter that was sent on a date in February 2013 to Eircom's Chief Medical Officer.

We commenced the investigation of the complaint and we asked Eircom to respond to the access request without further delay. We were informed by Eircom that it had already provided the data subject with a copy of the letter that was the subject of his access request, and it subsequently provided us with a copy of its response to an access request. However, on further inspection of Eircom's response to that access request, it was unclear to us that the response was in relation to the particular access request that was the subject of the current complaint as the response issued to the data subject prior to the date of his access request. We asked Eircom to review the matter. Eventually, on 2 May 2014, we received an email from Eircom enclosing a copy of the response of that date to the data subject's access request of 22 September 2013, supplying a copy of the document that the data subject had sought access to.

The complainant asked for a formal decision of the Data Protection Commissioner on his complaint. In making his decision, the Commissioner formed the opinion that Eircom Limited contravened Section 4(1)(a) of the Data Protection Acts by failing to supply the data subject with a copy of his personal data in response to his access request submitted on 22 September 2013 within the statutory period of 40 days. This contravention occurred when Eircom Limited released a copy of the data subject's personal data to him on 2 May 2014 – which was outside the statutory period of 40 days.

As outlined elsewhere in this annual report, over half of the complaints received by this Office in 2014 were made by data subjects who experienced difficulties in accessing their personal data. One common theme that emerges in many of these complaints is lateness on the part of the data controller in processing the access request. The Acts lay down a period of 40 days for compliance with an access request and if this is not met, as in the case outlined above, the data controller contravenes the Data Protection Acts. The Office of the Data Protection Commissioner is very concerned about the prevalence of this particular contravention. In some instances, the data controller fails to even acknowledge receipt of the access request within the 40-day period. This means that the requester has no idea whether their access request is being dealt with or ignored. There have been many instances where the data controller has taken no action whatsoever in terms of processing the access request until this Office commences an investigation on foot of receiving a complaint from the data subject. Clearly, that is an undesirable situation. Data subjects have a statutory right to access their personal data held by a data controller by the simple means of submitting an access request, and the data controller has a statutory obligation to comply with that request within 40 days. A data subject should not have to resort to the extra step of lodging a complaint with the Office of the Data Protection Commissioner in order to have their statutory right of access enforced. Unfortunately, as the complaint statistics reveal, far too many data subjects are experiencing barriers and access-denying tactics on the part of data controllers.

In the above case, the data subject's right of access was severely delayed. There is no justification for such a lengthy delay in any circumstances. Such a delay is particularly unacceptable in a situation where the requester simply sought a copy of personal data contained in one relatively recently created letter and where the data controller is a large telecommunications company that is well aware of the Data Protection Acts and receives and processes subject access requests on a regular basis. Eircom is the subject of several data-protection complaints every year across a range of issues, many of which relate to access requests. The Office of the Data Protection Commissioner expects to see a marked improvement in that company's data-protection performance in the near future, particularly in the context of processing subject access requests in a timely manner.

Case Study 12: Third-Level Student Data Appeared on Third-Party Website

The Office received a notification from a data controller, in accordance with the Personal Data Security Breach Code of Practice. The notification alerted the Office to the fact that data relating to a large number of students had been discovered on a website that was unrelated to the data controller. The data related to the 2010 academic year.

The Office began an investigation of the matter. The data controller advised the investigation team that the information disclosed on the website included the name, email address and password of the student. The investigation team confirmed that there was no financial or sensitive data involved.

The data controller engaged an external security company to carry out its own investigation into the security breach.

Due to the passage of time, there were no server logs showing when or by whom the data had been uploaded to the website. However, the data controller was able to identify that the data published matched a file created for testing purposes in mid-2011. This file was then sent to a third-party service provider who was engaged in developing a management system for the data controller. The file was sent via unsecured email.

The third-party service provider informed the data controller that while there was a relationship between their staff and the website on which the data was published, they had conducted a very thorough review of the matter and could find no evidence to show that the file had been posted onto the website due to an act of omission on their part.

Our evaluation of the information showed that the data controller, when creating student accounts, used generic passwords when generating the student accounts. The password was the date of birth of the student. While students could change their passwords, they were never advised to change them.

While it could not be determined exactly how the data appeared on the website, it was evident that there had been a breach of the Data Protection Acts, in that appropriate security measures were not in place to prevent the unauthorised disclosure of personal data.

Our investigation also found that the use of live data for testing purposes was not in accordance with data-protection best practices. Where live data is being used by an organisation for testing purposes, there would have to be a strong justification for such use and we were not aware of any justification applicable in this particular case. The Office recommended that the data controller cease the use of live personal data for testing and either anonymise the data or create a fictitious data set for testing purposes.

The transmission of such student data via an unsecured channel is also inconsistent with the Data Protection Acts. It was found that, during the development of the management system, personal data, including passwords, was exchanged between the data controller and the service provider, using an unsecured channel. The data controller advised my Office of the fact that they now transmit such data via a secure mechanism. The Office recommended that this mechanism be brought to the attention of all staff.

Another issue discovered during our investigation that caused great concern was the use of a generic password. The fact that the date of birth of the student was assigned as their password meant that any individual who had access to the date of birth of another student could access the user account of that student. The Office recommended that the data controller communicate with students, advising that they change their password and that the new password be a minimum of 12 characters and include upper- and lower-case characters, numerals and special characters, such as a symbol or punctuation mark.

Case Study 13: Data Controller Discloses Personal Data to Business Partner

The Office received notification from a data controller advising that an email had been issued to a business partner which included personal data that should not have been disclosed.

The data controller advised the Office that it had entered into a business agreement with a third-party company to provide anonymised data to allow for a feasibility assessment of a proposed business venture. An email was issued to the third-party company which included the names of individuals in addition to the agreed anonymised data. This allowed for the third-party company to identify the individuals involved.

The data controller, in notifying this Office, stated that the third-party company had provided assurances that the data had been deleted.

The Office commenced an investigation of a data-security breach, under Section 10 of the Data Protection Acts.

Given the nature of the data involved and additional information received by a third party, this Office decided to visit the premises of the third-party business partner to satisfy ourselves that the data had been deleted and not further processed.

An investigation team, using our powers under Section 24 of the Data Protection Acts, arrived unannounced at the premises of the business partner. The team obtained documents in relation to the business agreement; these showed that only anonymised data had been sought. The team also obtained reports that had been created on foot of the receipt of the personal data. It was evident from these reports that, while personal data was available to the third party, it had not been used in the preparation of the reports and had no impact on the reports.

The team then examined the computer systems of the company and discovered

several instances of the email it had received which contained the personal data.

The Commissioner felt it appropriate to issue an Enforcement Notice to the third-party company, requiring them to engage an external IT security company to delete any and all copies of the personal data it had received. The IT security company was to provide my Office with a report on the completion of the work. This report was duly received and this Office was satisfied that all copies of the personal data had been securely deleted.

The investigation found that personal data had been disclosed without consent or a legal basis. The investigation also noted that non-business related email accounts had been used by members of staff of the data controller in the conduct of business matters. The data controller was advised to prevent the use of non-business email accounts as the data controller could not control any data that would be transmitted through these non-business accounts.

Case Study 14: Employee of Financial Institution Resigns Taking Customer Personal Data

The Office received a notification from a data controller, in accordance with the Personal Data Security Breach Code of Practice. The notification stated that an employee had tendered their resignation and the data controller then discovered that the employee had emailed a spreadsheet to their personal email account prior to their resignation. The spreadsheet contained details of customers, including their employment details, salaries, contact details and medical consultant.

The data controller provided the name and home address of the employee.

The Office was also contacted by the umbrella organisation of the data controller seeking assistance on how to advise their member.

The Office verified, through the Companies Registration Office, that a business was operating from the home address of the employee. We then contacted the employee on the basis that they were now operating as a data controller in their own right. We sought clarification from the employee as to the consent they had to process any personal data they obtained from their previous employment.

The employee advised the Office that, as part of their employment, they were asked to use their own laptop and personal phone for all business dealings. The employee also advised that they had not yet started canvassing for clients. The employee also confirmed that they had deleted all the personal data they held in relation to their previous employment.

We also engaged with the data controller who had made the notification in relation to the security procedures that were in place to protect customer data in its possession. The Office noted that the employment contract contained appropriate data-protection clauses. However, of concern was the fact that employees were using their own equipment for business purposes. In such circumstances, the data controller has little or no control over that data held on personal equipment.

The data controller introduced further procedures and policies on foot of the issue to prevent a repeat of this type of incident, including the introduction of software to password protect any data records being emailed. Furthermore, all employees must sign an undertaking on termination of employment that all data has been returned and will not be further processed.

Case Study 15: Theft of Unencrypted Laptop

The Office received a data-security breach notification during the year from a medical professional relating to a stolen laptop.

The notification advised that the laptop was password protected, but not encrypted. The notification also advised that the data stored on the laptop related to a medical study that was undertaken in 2009 and included audio files of interviews carried out with the study subjects which contained limited information. It was determined that a file listing the subjects of the study contained an ID number rather than the name of the individual. However, a further file that correlated the ID number with the subject name was also stored on the laptop. This file was also password protected.

It was noted that, before the study began, approval was obtained from the relevant Ethics Committee that covered the storage of data.

This Office advised the data controller of our guidance in relation to the notification of the affected individuals. In this particular case, the data controller advised the Office that it was of the view that notification to affected individuals would cause more distress than help to the affected individuals. This view was offered by the relevant medical professional overseeing the project. This Office must note the opinion of a medical professional who has a professional relationship with the affected individuals. We assume this decision is taken weighing the potential effects of an unauthorised disclosure of this data against the potential distress of the individual being notified of the security breach.

The Office, however, noted that laptops are now being encrypted. This case highlights the fact that data-protection considerations need to be constantly monitored. What may have been an acceptable standard five years previous may not now be acceptable, and security arrangements must be periodically reviewed.

Case Study 16: Compromise of Adobe Network

Adobe Systems Software Ireland Ltd notified this Office in October 2013, in accordance with the Personal Data Security Breach Code of Practice, of a data-security breach regarding an unauthorised access to their systems. Personal data was compromised and the attacker also took Adobe software source-code elements.

Two data controllers were affected: Adobe US and Adobe Systems Software Ireland Ltd (Adobe Irl). We engaged in a coordinated

investigation with the Office of the Privacy Commissioner of Canada and we were co-joined in our investigation by the Office of the Australian Information Commissioner.

Nature of Data Compromised

Adobe Irl created three classifications of individuals affected:

- Payment-card users, i.e. those whose encrypted payment-card numbers were accessed during the breach. The data involved was encrypted payment-card data – approximately 3.65 million payment cards (1 million controlled by Adobe Irl) relating to approximately 3.1 million individuals.
- Active users, i.e. those who had logged in to Adobe systems at least once in the two years prior to the discovery of the breach. The data involved was: email address and current encrypted password – 41 million (reduces to 33 million, as 8 million email notifications were undeliverable) (20.5 million controlled by Adobe Irl).
- Non-active users, i.e. those who had not logged in to Adobe in the two years prior to the discovery of the breach. The data involved was: email address and current encrypted password – 71 million (reduces to 46.5 million due to 25 million email notifications undeliverable) (28.5 million controlled by Adobe Irl).

How the Breach Occurred

The attack was a sophisticated and sustained intrusion of Adobe's computer systems. Attackers identified and removed data from a backup server that stored the compromised data described above. Adobe states it has no evidence to show that unencrypted card details were taken. Forensic consultants engaged by Adobe supported this conclusion.

When Adobe learned of the security breach, they began an investigation of the cause of the issue and also initiated a series of measures including the following:

- Disconnected the impacted database server from the network
- Blacklisted IP addresses from which the attacker accessed their systems
- Reset passwords for all potentially affected users (including active, non-active)
- Changed passwords for relevant administrator accounts
- Notified the banks processing customer payments for Adobe, so they could work to protect customers' accounts
- Reported the breach to law-enforcement authorities
- Employed a third-party company to conduct an investigation of the cause of the security breach of its systems and to identify what data may have been compromised
- Took actions to reduce the risks related to the theft of certain source-code elements
- Issued notifications to affected individuals, beginning on 3 October 2013, which alerted customers to the security breach

Passwords

At risk: the attacker posted some data that was exfiltrated on a website and included the email address and encrypted password of certain Adobe users. A number of research articles have demonstrated that some passwords have been deciphered by reference to password hints and repeated passwords (i.e., the same password used by more than one user). One article highlighted an organisation that had checked the compromised usernames and deciphered passwords against its own platform and found a significant number of these credentials would have worked on its own platform. The organisation contacted some of its affected users, alerting them to the issue, and also confirmed the scenario to this office. At issue here is that while Adobe enforced a password change on its own site and advised users to change their passwords elsewhere, it is evident that not all users followed such advice.

Hints: Parts of the data exfiltrated by the attacker were the password hints of a small percentage of users. These hints were stored in clear text and associated with the username (email address). This information, along with an analysis of the encrypted passwords, will allow for the identification of certain simple passwords. However, as previously noted, Adobe reset the passwords for all impacted users.

Storage: The Office queried why passwords were stored in one system in an encrypted manner rather that hashed and salted. Encrypted passwords can be unencrypted, which would allow a data controller to see the passwords of users, or attackers, if they gained access. Adobe stated it was actually hashing and salting passwords within a new system for a number of years prior to the discovery of the security breach, but decided to also keep the database in the old system as a backup measure in case of issues with the new system. Passwords in the old system's database had been encrypted.

Retention of Card Data with Customer Records

Customers who used payment cards to purchase Adobe products or services had their card details (encrypted) stored with the customer account within one particular system. Card numbers have now been replaced with a token system. This process began prior to the discovery of the security breach and was completed shortly thereafter. The token, which is encrypted, represents the payment-card number within the customer record and Adobe systems transmits the encrypted token to a third-party service provider, whose systems are located outside Adobe's network, for payment processing.

Notifications to Affected Individuals

Adobe provided the Office with a list of when they notified each class of affected individuals and the relevant notification. In addition, Adobe publicly announced the 2013 breach in posts on its website, which included discussion of the theft of source code. The various notifications did advise individuals to monitor their credit-card statements and change their password if it was used on another site.

When we queried why notifications did not issue to those individuals where only contact details were compromised and did not include password or payment-card data, Adobe replied that it believed that notice in this scenario would lead to over-

notification and notification fatigue and that there is not a significant risk of harm with respect to a compromise of this type of data element. The Code of Practice recommends that affected users are notified, so that each affected individual can consider the consequences for themselves and take appropriate measures.

This Office would expect that if a similar incident were to occur in the future, Adobe, or any other data controller, would automatically include all individuals for whom personal data had been compromised in its notification process.

Conclusion and Findings

Adobe fully cooperated with our investigation of the security breach reported to us on 2 October 2013. Adobe took appropriate action on discovery of the attack to prevent further access to their systems as required under Section 2(1)(d) of the Data Protection Acts 1988 and 2003. It also enforced a password change for its users to protect against unauthorised access to account data. Adobe's quick reaction on learning of the security breach prevented the attacker from exfiltrating unencrypted payment-card details.

Adobe's transitioning from the use of encrypted passwords in the old system to the use of hashed and salted passwords in the new system could have been achieved more effectively and expeditiously than was the case. Of concern to those users who provided password hints, Adobe stored these in plain text rather than in an encrypted format, some of which have been compromised.

This Office is cognisant of the fact that data controllers such as Adobe will always be a target for attackers and new attack methods are constantly being devised.

This Office found that Adobe was in breach of Section 2(1)(d) of the Acts by failing to have in place appropriate security measures to protect the data under its control, despite its documented security programme. It was also recommended that Adobe engages a third party to carry out an independent review of its systems.

Adobe has since put in place substantial improvements in its security protocols, practices and procedures, and this Office is satisfied that it now has appropriate procedures in place to minimise the possibility of a similar security breach in the future.

PRESENTATIONS

During 2014 the Commissioner and staff of the Office gave presentations to the following organisations:

Educational
Árdscoil na Tríonóide, Athy x 2
Athy College x 2
Árdscoil na Tríonóide, Athy x 5
National Council for Special Education
Student Legal Convention
School of Computer Science and Statistics
National Induction Programme for Teachers (NIPT) x 2
St Pauls Secondary School Monasterevin x 2
Gael-Choláiste Chill Dara x 3
NCSE
Waterford Institute of Technology

Voluntary
Cork Deaf Society

Commercial
Institute of Chartered Secretaries and Administrators
Irish Computer Society
Irish Security Industry Association

Telecommunications
Telecommunications Industry Federation

Insurance
PIAB

Health Sector
RCSI-Clinical Research Nurses Course
Irish Dental Association
Occupational Health Nurses Association of Ireland

International
Computers Privacy and Data Protection Conference
International Association of Privacy Professionals
US Embassy Annual Economic Conference
EUROFORUM Berlin
Stanford E-Commerce Conference
German Bar Association
International Association of Privacy Professionals x 2
Occupational Health Nurses Association of Ireland

Legal
Matheson Solicitors
IBEC Employment Law Conference
Bar Council of Ireland

Financial
Comhar Creidmheasa Cholm Cille Teo

Mixed Seminars
MBA Organisation
TAIEX Brussels
Taking Care of Business x 4
US Embassy Annual Economic Conference
Fingal Senior Citizens Forum
C & I Privacy Forum UK
Institute of International and European Affairs
Iron Mountain

Government/Agency
Industrial Development Authority
Civil Service Employee Assistance Service
Institute of Public Administration
Adoption Authority of Ireland
Defence Forces Headquarters
Public Appointments Service (PAS)
Department of Public Expenditure
Department of Foreign Affairs

REGISTRATIONS STATISTICS

Certain categories of data controllers (major holders of personal data) are legally bound to register with the Data Protection Commissioner on an annual basis. However, every data controller, regardless of whether they are required to register with this Office, are bound by the data-protection responsibilities set out in the Data Protection Acts 1988 and 2003. Equally, registration with this Office is a separate legal process and should not be interpreted as automatically deeming an organisation to be fully data-protection compliant by virtue of having their registration entry up to date.

The total number of register entries in 2014 was 6,196. This figure can be broken down into the following categories:

Financial and credit institutions	544
Insurance organisations	333
Persons whose business consists wholly or mainly in direct marketing, providing credit references or collecting debts	94
Telecommunications/ internet providers	47
Health sector	1,941
Pharmacists	1,130
Miscellaneous	952
Data processors	1,155

Total number of registration entries

2012	2013	2014
5,338	5,778	6,196

In 2014, the number of organisations registered increased by 418, approximately 7%. This increase arose due to a targeted awareness campaign on credit unions and physiotherapists.

ACCOUNT OF INCOME AND EXPENDITURE

Account of receipts and payments in the year ended 31 December 2014

	2014	2013
Receipts	**€**	**€**
Moneys provided by the Oireachtas	2,274,438	1,960,999
Fees	714,697	647,997
Other receipts	Nil	Nil
Receipts total	**2,989,135**	**2,608,996**
Payments		
Staff costs	1,654,900	1,627,911
Establishment costs	73,115	131,630
Legal and professional fees	522,145	179,050
Audit fees	4,117	Nil
Miscellaneous expenses	20,161	22,408
Payments total	**2,274,438**	**1,960,999**
Actual payment of receipts for the year to the Vote for the Office of the Minister for Justice and Equality	414,347	626,536
Receipts payable to the Vote for the Office of the Minister for Justice and Equality at year end	300,350	21,461
Total	**2,989,135**	**2,608,996**

*The figures for 2014 outlined above are still subject to audit by the Comptroller and Auditor General. The final audited accounts will be presented to the Minister for Justice and Equality for presentation to the Oireachtas.

ENERGY REPORT

Overview
The Data Protection Commissioner's Office is part of a building that was built in 2006. We occupy the first floor of the building, with a floor area of 13.38 square metres. Currently, 31 members of staff are accommodated in this area.

In 2014, the sources of the main usage of energy in the Office were gas and electricity for heating, lighting and other uses.

In 2014 the energy rating for the building was C1.

Actions Undertaken
The Office has participated in the SEAI online system in 2014 for the purpose of reporting our energy usage in compliance with the European Communities (Energy End-Use Efficiency and Energy Services) Regulations 2009 (SI 542 of 2009).

The annual energy usage for the Office for 2014:

Usage	**80,574**
Non-Electrical	33,124kWh
Electrical	47,450kWh

The Office has continued its efforts to minimise energy usage by ensuring that all electrical equipment and lighting are switched off at close of business each day.

During 2014, the office concluded the process of introducing an extension to our existing permanent gas-heating system; this has obviated the need to use portable heaters. All light bulbs have now been replaced with energy-saving bulbs throughout the Office. We will continue to explore further ways of reducing energy usage.

NOTES

NOTES

Canal House
Station Road
Portarlington
Co. Laois
Ireland

Lo Call Number 1890 252 231
Telephone +353 57 868 4800
Fax +353 57 868 4757
E-mail info@dataprotection.ie

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner